UNIVERSITY OF KWAZULU-NATAL | INYUVESI YAKWAZULU-NATALI | COLLEGE OF HUMANITIES
NATIONAL INSTITUTE FOR THE HUMANITIES AND SOCIAL SCIENCES
SABTT South African BRICS Think Tank

BRICS

# PEACE, SECURITY, AND ECONOMY RESEARCH INTERSECTIONS

Editors: Professor Nirmala Devi Gopal, Professor Gert Kruger, and Dr. Sandhya Maharaj

*Alter*nation African Scholarship Book Series, Volume #21

# *Alter*nation African Scholarship Book Series (AASBS)


## General Editors

Nhlanhla Mkhize; Relebohile Moletsane; Nobuhle Ndimande-Hlongwa; Sarah Mosoetsa; Stephen M. Mutula; Labby Ramrathan; Johannes A. Smit

---

## Lead-Editors

Nyna Amin *University of KwaZulu-Natal;* Vivienne Bozalek *Cape Peninsula University of Technology;* Denzil Chetty *University of South Africa;* Rubby Dhunpath *University of KwaZulu-Natal;* Bekithemba Dube *Central University of Technology*; Mari Haugaa Engh, *Norwegian University of Science and Technology*; Dipane Hlalale *University of KwaZulu-Natal;* Maserole Kgari-Masondo *University of South Africa;* Simangaliso Kumalo *University of KwaZulu-Natal;* Sam Lubbe *Mangosuthu University of Technology;* Sadhana Manik *University of KwaZulu-Natal;* Cheryl Mohamed Sayeed *University of KwaZulu-Natal;* Herbert Moyo *University of KwaZulu-Natal;* Oliver Mtapuri *University of KwaZulu-Natal;* Priya Narismulu *University of KwaZulu-Natal;* Maheshvari Naidu *University of KwaZulu-Natal;* Joram Ndlovu *University of KwaZulu-Natal;* Edmore Ntini *University of KwaZulu-Natal;* Beatrice Okyere-Manu *University of KwaZulu-Natal;* Kunle Oparinde *Durban University of Technology;* Michael Samuel *University of KwaZulu-Natal;* Federico Settler *University of KwaZulu-Natal*; Upasana Gitanjali Singh *University of KwaZulu-Natal*; Lilian Siwila *University of KwaZulu-Natal.*


*Alter*nation research groups have made decisive and far-sighted knowledge production contributions in the interdisciplinary Arts and Humanities arena for more than twenty-five years. From 2020, it adds the *Alter*nation African Scholarship Book Series (AASBS) to its research outputs system. Via its incisive thematically-focused inter-, multi-, and trans-disciplinary, as well as digitally-informed, research approaches, the AASBS not only advances the frontiers of knowledge in Africa's institutions of Higher Learning in designated focus areas, but also critically generates scholarship of, by and with the people(s) of our continent. Historically the research draws on the rich traditions of interactive African intellectualisations, from its earliest civilisations, through struggles for liberation and freedom, to independence and growth. It opens up future epistemic opportunities through intellectual initiative and resourcefulness, while critically contributing to the international advancement of knowledge on all relevant levels. Contributing to research-led constructive, transformative and substantial discourse development in our programmes and disciplines, it also aims at impacting the wellbeing of our people foundationally and all-inclusively in the present. All forms of scientific and social challenge which Africa's societies and communities face, need to be problematised and researched in the Arts and Humanities, in the interest of cooperative and conscientious responsible knowledge generation and foundational conceptual and methodological research impacts. We serve the hopes and aspirations of the people of Africa.

AASBS is committed to the highest levels of inclusive, factually correct and critical, socially-responsive and socially-accountable evidence-based research analyses and outputs. Each chapter is reviewed by at least two independent peer reviewers. Through its editing and peer-review system, each volume also builds research leadership, research expertise, and interactive research acumen, capacity and capabilities.

*A list of published and upcoming titles follows overleaf*

# *Alter*nation African Scholarship Book Series (AASBS)

Ramrathan, L., N. Ndimande-Hlongwa, N. Mkhize & J.A. Smit (eds.). 2020. *Re-thinking the Humanities Curriculum in the Time of COVID-19. Volume #01.*

Ndimande-Hlongwa, N., L. Ramrathan, N. Mkhize & J.A. Smit (eds.). 2020. *Technology-based Teaching and Learning in Higher Education during the Time of COVID-19. Volume #02.*

Mkhize, N., N. Ndimande-Hlongwa, L. Ramrathan & J.A. Smit (eds.). 2020. *Teaching and Learning in Higher Education in the Time of COVID-19. Volume #03.*

Smit, J.A., N. Mkhize, N. Ndimande-Hlongwa & L. Ramrathan (eds.). 2020. *Learner and Subject at the Dawn of Digital Research-Led Teaching and Learning in the Time of COVID-19. Volume #04.*

Manik, S. (ed.). 2020. *From High-risk Sports to Sports as High Risk: Crisis, Capitulation and Creativity during COVID-19. Volume #05.*

Kumalo, S.R., C. Lynch, A.B. Bangirana & C. Kemedjio (eds.). 2021. *Critical Perspectives on Governance, Religion and Humanitarian Aid in Africa. Volume #06.*

Singh, U.G., P.S. Reddy, M.W. Phiri & P. Appavoo (eds.). 2021. *Global Trends in Management, IT and Governance in an E-World. (E-MIG 2019 International.) Volume #07.*

Amin, N. & R. Dhunpath (eds.). 2021. *(Re)Learning to Teach in Contexts of Crises. Volume #08.*

Bob, U. (ed.). 2022. *The COVID-19 Pandemic: Impacts of the Corona Virus on Sport and Society. Volume #09.*

Moran, S. 2022. *Primitive Times. Volume #10.*

Singh, S.B. (ed.). 2022. *Indians in South Africa: Perspectives from 1860 to the 21st Century. Volume #11.*

Ramrathan, L., R. Hoskins & V.S. Singaram (eds.). 2022. *Assessment through Digital Platforms within Higher Education Studies. Volume #12.*

Jain, P., N. Mnjama & O. Oladokun (eds.). 2023. *Information and Knowledge Management for Social, Economic and Political Development. Volume #13.*

Samuel, M.A. & H. Mariaye 2023. *Transforming Postgraduate Education in Africa. Volume #14.*

Mutula, S.M. (ed.). 2024. *The Diasporean I: The Southern African Perspectives. Volume #15.*

Mutula, S.M. (ed.). 2024. *The Diasporean II: Perspectives from Beyond Southern* Africa. Volume #16.

Patrick, H.O. & N.E. Khalema (eds.). 2024. *Migration, and Identity Construction in Africa: Implications for Policy and Practice. Volume #17.*

Patrick, H.O. & N.E. Khalema (eds.). 2024. *Migration, and Integration in Africa: Implications for Policy and Practice. Volume #18.*

Smit, J.A., D. Gengan, E. Gandhi, C. Carson, R. Saleh, P. Gollanapalli, S. Sonty (eds.). 2025. *Mahatma Gandhi, Nelson Mandela & Martin Luther King Jr. Peace and Justice for All – Mobilizing for Nonviolent Change (Ahimsa): Keynote Papers. Volume #19.*

Smit, J.A., D. Gengan, E. Gandhi, C. Carson, R. Saleh, P. Gollanapalli, S. Sonty (eds.). 2025. *Mahatma Gandhi, Nelson Mandela & Martin Luther King Jr. Peace and Justice for All – Mobilizing for Nonviolent Change (Ahimsa): Youth Symposium. Volume #20.*

Gopal, N.D. & G. Kruger & S. Maharaj 2025. *BRICS Peace, Security & Economy Research Intersections. Volume #21.*

Mkhize, N. & S. Ehiane (eds.). 2025. *Aspects of African Scholarship in the Humanities and Social Sciences. Volume #22.*

# *BRICS*
# *Peace, Security, and Economy*
# *Research Intersections*

Editors
Nirmala Devi Gopal,

Gert Kruger

AND

Sandhya Maharaj

2025

NATIONAL INSTITUTE FOR THE HUMANITIES AND SOCIAL SCIENCES

CSSALL
Durban

SABTT South African BRICS Think Tank

Published in 2025 in South Africa

CSSALL Publishers (Pty) Ltd
c/o POSTNET SUITE 158
Private Bag X9118
Pietermaritzburg
KwaZulu-Natal
3200

Email: cssall123@gmail.com
Editor-in-Chief: Prof J.A. Smit
University of KwaZulu-Natal
Email: smitj@ukzn.ac.za

*Alter*nation African Scholarship Book Series Volume #21
© CSSALL Publishers (Pty) Ltd

Title: *BRICS Peace, Security, and Economy Intersections*
Editors: Nirmala Devi Gopal, Gert Kruger & Sandhya Maharaj

ISBN: 978-0-9869938-0-0.
DOI number: https://doi.org/10.29086/978-0-9869938-0-0/2025/AASBS21

Cover design: Corporate Relations Graphic Design, University of KwaZulu-Natal

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the copyright holder and publisher.

CSSALL has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this volume, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Printed and bound by Print Connection, Tel (031) 202-7766

# Preface

Sponsored by the National Institute for the Humanities and Social Sciences (NIHSS), the University of KwaZulu-Natal and the South African BRICS Think Tank, organised the multidisciplinary *2018 Peace and Security Symposium*, and the *2024 International Conference on the Nexus between Security and Economy.* For this volume, of the *Alter*nation African Scholars Book Series, Nirmala Devi Gopal and Gert Kruger, together with Sandhya Maharaj, the conference organisers, brought together some seminal papers from these events, titled, *The BRICS Peace, Security and Economy Intersections.*

The BRICS nations – (Brazil, Russia, India, China, and South Africa) – represent a significant geopolitical and economic force on the global stage. As a collective, BRICS represent the interests of these nations themselves as well as the developing world more broadly speaking. BRICS also aims to promote and mobilise for peace and security as well as for security and viable and constructive economic engagements and development in and for the BRICS nations, as well as worldwide.

Beyond their geopolitical initiatives for peace and justice internationally, the BRICS nations' additional main focus is on their economic prominence and competitiveness, and especially their emerging leading roles in economic development globally. In their developing framework, BRICS also share complex security challenges and risks that intersect with their economic objectives, with regard to their cybersecurity over a broad front, citizens' financial and medical security, good governance and human rights, the global drug trade, unemployment in especially Africa, trade and institutional investment, energy, intelligence, and psychological security, amongst others. As such, the evolving dynamics within the BRICS framework demand a nuanced understanding of the interplay between security studies and economic imperatives, that provides a framework for secure economic development and the fostering of economic resilience.

So, in response to these realities, the *2018 Peace and Security Symposium* deliberated seminal research focuses on the role of BRICS at the global and United Nations levels; on matters related to African continental, and Indian ocean maritime security; and on BRICS leadership concerning the post-Western era, the promotion of peace operations, and especially in the de-escalation of armed conflict and cybercrime internationally.

Subsequently, the *2024 International Conference on the Nexus between Security and Economy* addressed the intersection of security studies

and economic objectives within the BRICS Framework. The conference delved into the intricate interplay between security challenges and economic imperatives within the framework of the BRICS nations. It provided a platform for scholars, policymakers, practitioners, and stakeholders to engage in critical discussions, share insights, and explore innovative approaches toward understanding and addressing the complex dynamics at the intersection and articulation of security and economic priorities and challenges, within the BRICS context.

Some of the seminal papers addressed the security problematics and interventions related to regional and domestic cybersecurity that include,

- social media;
- governance, democracy, human rights, the rule of law and social dialogue, as essential foundations for peace and security in an expanded BRICS, including the countering of transnational cybercrime;
- financial matters related to economic integration in the BRICS nations; and
- BRICS investment, and economic aspects related to on-, and off-shore energy generation security, and environmental security;
- challenges related to reliable intelligence gathering;
- psycho-social security at local and communal levels; and
- plans toward the global improvement and preparation for future health pandemics.

Since its founding on 16 June 2009, in Yekaterinburg, Russia, with South Africa joining on 24 December 2010, BRICS's influence worldwide has grown systematically. We are grateful that this volume makes a helpful contribution to the developing BRICS discourse and impacts, in key areas of cybersecurity and economics.

Prof. Johannes A. Smit
Professor of Religion and Social Transformation
Chair: College of Humanities Institute
University of KwaZulu-Natal
Pietermaritzburg & Durban
smitj@ukzn.ac.za

Prof. Nirmala Devi Gopal
Criminology & Security Studies
Department of Criminology & Forensic Studies
University of KwaZulu-Natal
Durban
Gopal@ukzn.ac.za

# Contents

*Johannes A. Smit* and *Nirmala Devi Gopal*
Preface ..... v

Contents ..... vii

Contributors ..... ix

*Nirmala Devi Gopal, Gert Kruger* and *Sandhya Maharaj*
Chapter 1: Editorial:
The BRICS Peace, Security, and Economy Research Intersections ..... 1

**THE 2018 BRICS PEACE & SECURITY SYMPOSIUM**

*Mosud Y. Olumoye* and *Stanley O. Ehiane*
Chapter 2: Cyber Terrorism and Cyber Security in
Contemporary Nigeria ..... 17

*E.A. Mantzaris*
Chapter 3: Corruption and Citizens' Financial Security in
Public Service Medical Schemes: The Case of South Africa ..... 35

*H.H.S. Viswanathan*
Chapter 4: Can BRICS Contribute to Global Peace and Security? ..... 54

*Isaac Luthuli*
Chapter 5: The Menace of Cybercrime, Cyber Security and
Regional Response: The Case of Africa ..... 71

*Kai Michael Kenkel*
Chapter 6: Brazil, South – South International Security
Governance and Peace Operations (2003 – 2016) ..... 101

**THE 2024 BRICS**
**SECURITY & ECONOMY NEXUSES CONFERENCE**

*Nirmala Devi Gopal*
Chapter 7: The Use of the Internet for Nefarious Security Purposes:
Policies, Developments and Challenges of Terrorist Content on
Social Media ..... 129

*Oluwafisayo Kaka*
Chapter 8: A Survey of Cybersecurity Issues in BRICS Countries –
A Systematic Review ..... 187

*Simbarashe Tembo* and *James Ndlovu*
Chapter 9: Fostering Good Governance and Human Rights in an Expanded BRICS: Challenges and Opportunities ..... 222

*Sandhya Maharaj*
Chapter 10: An Exploratory Study on the Transnational Illicit Drug Trade and its Dangers to BRICS Countries – A Scoping Review..... 240

*Nontyatyambo Pearl Dastile*
Chapter 11: Cooperation in Countering Transnational Crime ..... 265

*Shanya Reuben* and *Shaida Bobat*
Chapter 12: Youth Unemployment and the Threat to Peace and Security: The Case of South Africa ..... 281

*Nirmala Devi Gopal* and *Cresencia Nyathi*
Chapter 13: Social Dialogue as a Vehicle to Address Peace and Security: An Analysis of the BRICs Formal Declarations ..... 300

*Irina Yarygina* and *Vladimir Smirnov*
Chapter 14: Institutional Investors in Russia: Security Problems and Prospects ..... 329

*Gargi Sharma*
Chapter 15: India's Energy Security Vulnerabilities: Assessing Threats to Critical Offshore and Onshore Energy Infrastructure in the Indian Ocean..... 343

*Adebimpe Saheed Fagbemi* and *Nirmala Devi Gopal*
Chapter 16: From Global to National Views: Examining Intelligence Gathering as an Intelligence-curbing Policy: A Review Essay ..... 365

*Matshepo Matoane*
Chapter 17: Psychological Security – Exploring Community Engagement in Peacekeeping ..... 381

*Gert Kruger* and *Colleen Aldous*
Chapter 18: The Mistakes Made in Response to the COVID-19 Pandemic: How to Deal with Future Pandemics ..... 407

Acknowledgements ..... 449

# ꕥ Contributors ꕥ

**Professor Colleen Aldous** is an academic and researcher at the University of KwaZulu-Natal (UKZN) in Durban, South Africa, where she holds a full professorship in the School of Clinical Medicine. Her career is marked by a strong commitment to both advancing medical research and fostering academic excellence through the mentorship of postgraduate students across multiple disciplines.

Professor Aldous's work also extends into collaborative research that spans national and international boundaries. She has been involved in multidisciplinary studies that address contemporary health challenges – from optimizing surgical techniques and improving trauma care systems to informing public health policies during pandemics such as COVID-19. Notably, her involvement in the recognised analysis of evidence surrounding repurposed drugs (for example, ivermectin) has contributed to shaping clinical practice guidelines and policy decisions in healthcare.

Her contributions are not only recognised in academic circles but also through active participation in scientific discussions and interviews. She regularly engages with broader audiences through interviews and expert discussions, such as those featured on platforms like Pharmacy Update Online, where she provides insights into emerging medical therapies and the evolving landscape of healthcare research.

Beyond her research, Professor Aldous is dedicated to nurturing the next generation of clinicians and researchers. She actively mentors postgraduate students, guiding research projects that span across medical disciplines and ensuring that emerging scholars are equipped with the tools and knowledge to advance healthcare. Her expertise in curriculum development and pedagogy is reflected in her leadership roles within academic settings, where she champions ethical research practices and evidence-based teaching.

Overall, Professor Colleen Aldous stands out as an influential figure in modern medical research and education, making lasting contributions to both the academic community and public health. Her interdisciplinary approach and dedication to mentorship continue to drive advances in clinical medicine and health sciences. Aldousc@ukzn.ac.za; https://orcid.org/0000-0002-7199-9160

**Ms Shaida Bobat,** BA Hons (UCT), MA (UND), is a lecturer in Psychology in the School of Social Sciences at the University of KwaZulu-Natal. She lectures in modules on Counselling in the workplace, Identity, conflict and power, and critical theory, and Work and Health. Her research interests are Critical theory, disability, labour relations and qualitative narratives on workplace wellbeing. She has published with colleagues in the areas of qualitative research on Women's Work – Life Balance Over the Life Course, racial hierarchies of skill and experiences of affirmative action, turnover intentions of telecommunications staff, Psychology, work and Organizations, and Women Entrepreneurs in Mkhuzi – North Coast. bobats@ukzn.ac.za

**Professor Nontyatyambo Pearl Dastile** is a decolonial scholar, and Criminology Professor, an NRF Rated Criminology scholar, and has recently been appointed as a Director of Postgraduate Studies at Walter Sisulu University (WSU). She was formerly Chair of the Department of Criminology and Security Sciences at the University of South Africa, a position she has held since June 2014. Her career in higher education spans over 26 years, ten years of which have been spent at the University of South Africa, where she was first appointed in 2008 as a Senior Lecturer. Her tenure at the University of South Africa has been characterized by a commitment to diversity research, collaboration, and a focus on assessment and in seeking opportunities to work with academic affairs to ensure student success.

Before joining Unisa, Prof Dastile held teaching positions in various institutions in different capacities, including the University of Transkei (now Walter Sisulu University) as a Tutor and Junior Lecturer, University of Venda (Junior Lecturer), University of Pretoria (Lecturer), and Monash South Africa (Lecturer). Professor Dastile was a visiting scholar at Rutgers University in the United States, where she taught a Module on Women and Crime. She served on numerous university committees.

Professor Dastile obtained her Doctoral Degree from the University of South Africa in Criminology, her Masters in Criminology from the University of Pretoria, Honours in Criminology (cum laude) (WSU) and B.A. in Criminology from the same institution (WSU).
She has been involved in a leadership position for the past 7 years, as a Chair of the Department and now Director Postgraduate Studies.

Her research interests include gender and crime, the decolonial epistemic perspective, offender assessment and rehabilitative program-

ming, Pan African criminology, African-centred methodologies, and alternative research methodologies.
ndastile@wsu.ac.za; https://orcid.org/0000-0002-7903-9308

**Dr. Stanley Ehiane** obtained his PhD in International Relations from the University of KwaZulu-Natal. He obtained a Graduate Certificate in Introduction to Cybersecurity in Business, from the University of Colorado, a Certificate in the New Approach to Countering Terror and Countering Violent Extremism, from the University of Maryland, and a Graduate Certificate in Understanding 9/11 and what happened and how terrorism affects our World today from Stanford School of Public Policy, Duke University, United States. He is an active member of the African Studies Research Forum (ASRF). His research interest are in the fields of Terrorism, Counterterrorism, Climate Change, Migration and Refugees, Cybercrime and Cybersecurity, Gender in Peacebuilding, Violence against Women and hate Crime.
stanleyehiane@yahoo.com; https://orcid.org/0000-0001-6871-4526

**Dr. Adebimpe Saheed Fagbemi**, Department of Criminology and Forensic Studies, University of Kwa-Zulu Natal, Durban, Republic of South Africa, and holds a Doctor of Criminology and Forensic Studies, College of Humanities, University of KwaZulu-Natal.
adebimpefagbemi@yahoo.com https://orcid.org/0009-0007-1412-3588

**Professor Nirmala Devi Gopal** has an illustrious career spanning 38 years in the education sector. She currently leads the Department of Criminology and Forensic Studies and recently served as the acting director of teaching and learning in the College of Humanities, University of KwaZulu-Natal. Professor Gopal has vast experience in the field of quality assurance, particularly in the context of Quality Council for Trades & Occupations (QCTO) and South African Qualifications Authority (SAQA) regulations. Her extensive role in the Education, Training and Development Practices Sector Education and Training Authority (ETDP SETA) has given her a deep understanding of these regulatory bodies and the standards they uphold. Furthermore, her membership on the board of the ETDP has greatly honed her knowledge and skills in corporate governance. She has dedicated her career to advancing knowledge in criminology, and her teaching methods have inspired many students to pursue careers in Criminology. Her contribution to the field is valuable, and her expertise is highly sought after by both students and

professionals alike. She is a C2-rated NRF scholar and recipient of many research grants as a principal investigator. Her funding opportunities include those from the National Institute of Humanities and Social Sciences (NIHSS) and the National Research Foundation (NRF). gopal@ukzn.ac.za; https://orcid.org/0000-0002-5104-0083

**Oluwafisayo Kaka** is a cybersecurity enthusiast with four years of experience lecturing on computer architecture, networking, and cybersecurity principles. She holds multiple information technology degrees and industry-recognised security certifications while seamlessly integrating academic knowledge with practical expertise in cybersecurity and AI initiatives. Beyond academia, Oluwafisayo offers advisory services to businesses seeking to improve their security systems. She is also passionate about empowering individuals through her volunteer work with Software Carpentry workshops, where she instructs shell scripting for cloud computing. oluwafisayo.kaka@gmail.com

**Professor Kai Michael Kenkel** is Associate Professor at the Institute of International Relations at the Pontifical Catholic University of Rio de Janeiro (IRI/PUC-Rio) and Associate Researcher at the German Institute of Global and Area Studies in Hamburg. He was trained at the Graduate Institute in Geneva and at The Johns Hopkins University. He has taught at universities in Brazil, Canada, Germany and Geneva. Kenkel has published extensively on security issues, focusing most recently on humanitarian intervention and the Responsibility to Protect, as well as United Nations peace operations, focusing especially on Brazil's role therein. His recent publications have centered on the normative debates surrounding intervention.
kenkel.iri@gmail.com; https://orcid.org/0000-0003-4356-9304

**Professor Gert (H.G.) Kruger** graduated from Potchefstroom University, South Africa, in 1996 under the supervison of Frans (F.J.C.) Martins and Attie (A.M.) Viljoen. His PhD lineage is traced back to Rudolf Criegee (Würtzburg) via Johan Dekker (Karlsruhe). The Dekkers introduced cage chemistry to South Africa, and Kruger actively pursues the synthesis, computational chemistry, and biotesting of various compounds in the Catalysis and Peptide Research Unit at UKZN. The Unit work on areas of drug-resistant bacteria, HIV, in-vivo imaging and TB. Kruger@ukzn.ac.za; https://orcid.org/0000-0003-0606-2053

**Isaac Luthuli** is a seasoned professional with a strong academic foundation in Social Science and International Relations. With experience in project coordination, effective communication, and academic mentorship, Isaac possesses a unique blend of knowledge and skills. Isaac holds a Master of Arts in International Relations from the University of KwaZulu-Natal. His research thesis focused on the role of the Southern African Development Community (SADC) and the Economic Community of West African States (ECOWAS) in facilitating continental integration. He also holds a Bachelor of Social Science Honours in International Relations from the University of KwaZulu-Natal, which he completed in 2013. His research topic for this degree was 'The Feasibility of "African Solutions to African Problems": Assessing the Role of the African Union in Kenya's Electoral Crisis (2007 - 2008)'. Additionally, Isaac holds a Bachelor of Social Sciences degree from the University of KwaZulu-Natal, which he completed in 2012. He matriculated from Lamontville High School in 2007.

Throughout his career, Isaac has demonstrated his versatility and adaptability by holding various roles in academic and public sector institutions. Isaac has experience as an Academic Mentor at the University of KwaZulu-Natal, where he worked from March 2013 to November 2014. He has worked as a Media Liaison Officer at the Kwa-Zulu Natal Department of Education from July 2014 to June 2015. He also worked as a Coordinator for Special Projects at the Department of Higher Education and Training (DHET) from August 2015 to February 2017. He also worked as an Academic Coordinator at Elangeni College, a position he has held since April 2019. Isaac has further increased his public sector experience by holding a role of being the Head of Ministry for various KZN Provincial Government Departments such as; KZN Department of Public Works, Human Settlements, Transport, Community Safety and Finance.

In addition to his professional experience, Isaac has held various leadership positions. He served as the Provincial Secretary of the Congress of South African Students (COSAS), the Branch Secretary of the Young Communist League of South Africa (YCLSA) in UKZN PMB Campus. Isaac has also chaired the Youth Desk Scottsville Area (Alexandra Police Station) from 2013 to 2014 and has been a member of the UKZN Students Services Council and the Central Student Representative Council (UKZN) responsible for Student Services. He also served as the Deputy National Secretary of the Young Communist League of South Africa (YCLSA) from 2014 to 2018 and

was a member of the YCLSA National Working Committee during the same period.

Isaac has been involved in various voluntary and community engagement activities. He has worked as an Academic Mentor at the College of Humanities, University of KwaZulu-Natal (UKZN) in 2014 and has been a Student Guide and Coordinator at UKZN Corporate Relations in 2012. Additionally, Isaac has interned at the KZN Christian Council in 2011 and has volunteered at the Lamontville Thembalethu Care Centre in 2009. In 2018, he presented a paper titled 'The Menace of Cybercrime, Cyber security and Regional response: The Case of Africa' at the BRICS Think Tank Seminar, National Institute for Humanities and Social Sciences (NIHSS), Parktown. He has travelled various countries such as; China, Russia, Greece, Egypt, Ghana and Ivory Coast to name the few. Isaac.Luthuli@Kzntransport.gov.za

**Dr. Sandhya Maharaj,** is a lecturer in the School of Law, College of Law and Management Studies, University of KwaZulu-Natal, and Attorney and Conveyancer of the High Court of South Africa). She has a special interest in substantive criminal law and criminal justice. She has served as a candidate Attorney at Legal-Aid South Africa and subsequently worked in private practice as a Conveyancer and as criminal defence Attorney. In 2017, she graduated with a PhD and thereafter served as postdoctoral research fellow at UKZN, School of Law, Pietermaritzburg. She currently lectures in modules on Specific Offences, Evidence, Civil Procedure and Advanced Criminal Lw (LLM). MaharajS2@ukzn.ac.za

**Professor Matshepo Matoane** is an Associate Professor of Psychology at the University of KwaZulu-Natal and a registered Clinical Psychologist. Her research interests include Afrocentric approaches to Psychology and psychotherapy, Community Psychology, Health Psychology, mental health and student support. She is also passionate about community interventions within under-resourced settings.
Matoanem@ukzn.ac.za; https://orcid.org/0000-0002-1824-384X

**Professor Evangelos A. Mantzaris** is retired professor of sociology and management, and current researcher at Mangosuthu University of Technology (MUT), Durban, South Africa. He completed an Honours in Political Science, Economics and Sociology with distinction at Panteios University, Athens, and a Masters in Sociology and a PhD at the University of Cape Town,

in South Africa. He has published 8 full scale books in English and Greek, and numerous peer-reviewed chapters in books, SAPSE journal articles, in peer-reviewed International Conference Proceedings, and has presented papers in over 70 national and international conferences. He received the award for most published professor at MUT in 2024. Mantzaris.Evangelos@mut.ac.za; https://orcid.org/0000-0003-0490-6953

**James Ndlovu** is a multi-disciplinary scholar with interest in politics, international relations, peace building, conflict transformation, diplomacy, religion, political theology and their intersections. He holds a PhD in Religion & Social Transformation, and a Masters in Conflict Transformation & Peace Studies, both from UKZN. He is also a graduate from the South African Theological Seminary. He is an experienced researcher, policy analyst and consultant.

**Dr. Cresencia Nyathi** is a dedicated scholar and advocate with extensive experience in human rights, community development, and administrative leadership across South Africa and Zimbabwe. Dr. Nyathi holds a Bachelor of Arts in Peace and Conflict Studies with a History minor (Cum Laude) from Solusi University, Zimbabwe. She earned a Master of Science in Public Administration with a specialisation in Peace Studies from Durban University of Technology, with her thesis focusing on reducing conflicts within rural women's Self-Help Groups in Hwange District, Zimbabwe. She also holds a Doctoral degree in Public Administration, specialising in Peace Studies, from Durban University of Technology, where her thesis investigated reducing youth participation in xenophobic violence in Durban. Additionally, she undertook a Post-Doctoral Fellowship in Criminology at the University of KwaZulu-Natal, focusing on peace and security, the BRICS, border security, and social dialogue.

Her scholarly interests include migration, community development, social cohesion, conflict resolution, and peacebuilding. She has contributed to the academic field with a book chapter published by Springer titled 'Collaborative Conflict Resolution: A Case Study of Women's Self-help Groups in North-Western Zimbabwe'. Additionally, her forthcoming book chapter, 'Utilising the School Club Approach to Mitigate School Violence: A Case Study of Africa Unite School Clubs', will be published by Routledge in May 2025. Another book chapter, titled 'Harnessing Community-based Solutions to Reduce Youth Participation in Afrophobic Violence in Durban,

South Africa', has had its abstract accepted as of February 2025.

Dr. Nyathi's career spans over a decade, reflects a deep commitment to fostering social cohesion, and the empowering of marginalised communities, as well as the enhancing of organisational effectiveness. Currently, she focuses on research, grant writing, monitoring, and evaluation at Africa Unite in Durban, South Africa. In this role, she is responsible for drafting project proposals, delivering reports to funders, overseeing monitoring and evaluation processes, analysing project data, and conducting research to guide program development.

Dr. Nyathi's career at Africa Unite includes previous positions such as Project Coordinator and Field Facilitator. These roles involved proposal writing, advocating for marginalised groups, conducting needs assessments, training peer educators, and facilitating community mediation dialogues. Previously, she served as a Project Officer at Ntengwe Community Development in Victoria Falls, Zimbabwe, where she empowered women through Self-Help Groups and provided leadership training. She also completed an internship at Sethule Orphans Trust, supporting youth empowerment programs and participating in bereavement counselling.

Beyond her work with Africa Unite, Dr. Nyathi has served as a National Social Cohesion Advocate under the Department of Sports, Arts and Culture. Her career demonstrates her unwavering commitment to promoting social justice and community development.

cresencia.nyathi@gmail.com

**Dr. Mosud Y. Olumoye**, Department of Computer Science & Mathematics, Mountain Top University, Nigeria, holds a Doctor of Philosophy in Information Systems and Technology 2018 (UKZN), a Master of Science in Information Technology (MSc) 2014, a Master of Information Technology (MIT) 2006, both from Nigeria, and a Bachelor of Engineering (Hons.) in Mechanical Engineering 1995. His areas of specialisation are ICT in education; e-Government /Management Information Systems; ICT for Development; Technology implementation and adoption; Cyber-security and digital forensic; Health informatics; Interdisciplinary; Information and knowledge management. He has also undergone training in Advanced Professional Courses in Cyber-Security from Security and Forensic Studies, Nigeria; Executive Managerial Course in Peace/Reconciliation and Security Studies from Advanced Peace and Reconciliation Centre of Nigeria; Master in Certified Ethical Hacking and Cybersecurity by ESkills Academy. He

teaches different courses in Cyber Security and Computer Science such as Fundamentals of Cyber Security, Introduction to Digital Forensics; Biometrics Security; Information Security Policy and Cryptography Techniques, Operating Systems, Computer Network, System Analysis and Design, Software Engineering etc. He is a member of the following cyber-security bodies: Professional member of Cyber Security Experts Association of Nigeria (CSEAN); Fellow, Cyber-Security and Forensic Studies, Nigeria; Member, Computer Forensics Institute and Certified Forensic Examiner of Computer Forensics Institute, Nigeria (CFIN) Now Chartered Institute of Digital Forensic of Nigeria. Also, a member of the Institute of Information Technology Professional South Africa. Mosud Olumoye is CompTIA A+ and Microsoft Certified Professional. His research interests are ICT in education; e-Government /Management Information Systems; ICT for Development; Technology implementation and adoption; Cyber-security and digital forensic; Health informatics; Interdisciplinary; Information and knowledge management.
yomosud@mtu.edu.ng; https://orcid.org/0000-0002-6584-6096

**Dr. Shanya Reuben,** MA (Wits), and PhD (UKZN), lectures in Career Psychology, Organizational Behaviour, and Organisational Development, in Psychology, in the School of Social Sciences. Her research interests are in the area of Career Psychology and Development within localized contexts, work and identity. She has published qualitative research on Women's Work – Life Balance Over the Life Course, for women in the retail industry, and the structured nature of racial hierarchies of skill, related to experiences of affirmative action in Industrial Psychology. She is also involved in Community based health and wellness interventions for disadvantaged schools and communities. reuben@ukzn.ac.za

**Ms Gargi Sharma**, is a PhD student in the Politics and International Relations Department, University of Shefield. Prior to joining the programme, she has worked with several wildlife conservation organisations in India, with a particular focus on the illegal wildlife trade. She is broadly interested in the intersection of wildlife conservation, and social justice and securitisation. Her research project is an extension of her professional experiences. Using the case study method, she researches rhino conservation in the Kaziranga-Karbi Anglong landscape in Assam, India. Her thesis aims to answer these questions: 1) How is conservation

practiced where competing claims over resources exist? 2) How is conservation negotiated in multi-governance structures? And 3) How does the politics of conservation overlap with the politics of sovereignty? gargi.sharma@cii.in

**AAmb. H.H.S. Viswanathan** is Distinguished Fellow at the Observer Research Foundation. Earlier, he was a member of the Indian Foreign Service for 34 years. He has a long and diverse experience in international relations and Diplomacy. His foreign assignments include Belgium, Zaire, Czechoslovakia, Germany, China, Italy, Cote d' Ivoire, USA and Nigeria. He was the Head of Mission (Ambassador/ High Commissioner) in Cote d'Ivoire and Nigeria with concurrent accreditation to Niger, Guinea (Conakry), Sierra Leone, Cameroon, Benin, Chad, Equatorial Guinea and Sao Tome and Principe. At the Headquarters in MEA, he has been Deputy Secretary (East Europe) and Joint Secretary (Administration). In the USA, he was Consul General of India in San Francisco with a consular jurisdiction over 14 States in the mid-West and West coast of the US. He has also experience in multilateral diplomacy. He represented India in the African Development Bank, International Fund for Agricultural Development (IFAD) and Food and Agricultural Organization (FAO). He was also Observer at the Economic Community of West African States (ECOWAS). He has participated in numerous Seminars/ Conferences/ Workshops and presented papers on issues connected with Africa, China, BRICS, IBSA and Global Governance. He has also co-edited the book *In Search of Stability, Security and Growth: BRICS and a New World Order*, published by ORF. Apart from Indian languages like Tamil, Malayalam and Hindi he speaks French and Italian. His hobbies include Golf, music and reading. hhsviswanathan@orfonline.org

**Dr. Simbarashe Tembo** holds a Bachelor of Laws (LLB), Masters of Law (LLM), and a PhD in Constitutional Law from the University of KwaZulu-Natal. He is currently conducting his post-doctoral work in the UKZN School of Law where he also teaches both undergraduate and postgraduate modules. His research interests are constitutionalism in Africa, international and regional law, migration law, and human rights. Dr. Tembo has several scholarly articles and book chapters published in local and international publications. He has previously presented papers at various international conferences and seminars. tembos@ukzn.ac.za;
https://orcid.org/0000-0001-7491-6765

**Prof. Yarygina Irina Zotona** is the Head of the Chair 'Economics and Banking', of the International Institute of energy policy and diplomacy of MGIMO under the Ministry for Foreign Affairs of the Russian Federation, Professional member of the International Committee of the Association of Russian Banks, member of the working group of the State Duma of the Federal Assembly of the Russian Federation, member of Dissertation Councils, member of the Association 'Analytics', Head of the Analytical department of the Eurasian consortium (EIAC), Member of the Board and Research Director of the National Committee on BRICS research. jiz4@yandex.ru; https://orcid.org//0000-0001-6393-5645

# Editorial

# Chapter 1: Editorial
# The BRICS Peace, Security, and Economy Research Intersections

**Nirmala Devi Gopal**
**ORCID iD: https://orcid.org/0000-0002-5104-0083**

**Gert Kruger**
**ORCID iD: https://orcid.org/0000-0003-0606-2053**

**Sandhya Maharaj**
**ORCID iD: https://orcid.org/0009-0006-2670-2547**

In an era of shifting global power dynamics, the role of multilateral alliances in maintaining peace and security has become increasingly vital. The BRICS coalition – comprising Brazil, Russia, India, China, and South Africa – has emerged as a significant player in global governance, advocating for a multipolar world order that fosters cooperation, economic stability, and diplomatic engagement. The Peace and Security Symposium, funded by the National Institute for the Humanities and Social Sciences (NIHSS) and hosted in Johannesburg, provided a platform for distinguished scholars and diplomats to critically assess BRICS' potential in shaping international peace and security.

At the symposium, the prominent ambassador, H.H.S. Viswanathan, Alexandra A. Arkhangelskaya, Kai Kenkel, Probal Ghosh, and Malte Brosig, explored the nuances of BRICS' role in conflict mediation, international peacekeeping, and cyber security. The symposium was structured around several key themes, which this book seeks to expand upon:

## 1 BRICS and the United Nations Security Council

Siphamandla Zondi's insights on BRICS cohesion in the UN Security Council highlighted the complexities of multilateral diplomacy. While BRICS nations

AASBS Volume #21 (2025) DOI: https://doi.org/10.29086/978-0-9869938-0-0/2025/AASBS21
Chapter DOI: https://doi.org/10.29086/978-0-9869938-0-0/2025/AASBS21/1 pp. 1 - 14

have made strides in advocating for more equitable representation in global decision-making, challenges remain in achieving a unified approach to security issues.

## 2 The Geopolitical Influence of BRICS in Peace and Security

Ambassador Viswanathan's keynote presentation addressed whether BRICS can be a stabilizing force in international conflicts. With diverse geopolitical interests, BRICS members bring unique perspectives to peace negotiations. However, their ability to act collectively remains a subject of debate.

## 3 Regional Perspectives on BRICS Security Contributions

*Russia's Perspective:* Alexandra Arkhangelskaya provided an analysis of Moscow's approach to peace and security within BRICS, emphasising Russia's strategic objectives in global conflict resolution.

*Brazil's Perspective:* Kai Michael Kenkel examined Brazil's contributions to peacekeeping operations, particularly in Latin America and Africa, and how BRICS can expand its peacebuilding role.

*African Maritime and Cyber Security Challenges:* Philani Mthembu, Francis Kornegay, and Isaac Luthuli explored the emerging threats of cybercrime and the security framework for the Indian Ocean region – a strategic area for BRICS maritime cooperation.

## 4 The Future of a Post-Western Global Order

Malte Brosig's presentation addressed BRICS' response to large-scale armed conflicts and its role in shaping a post-Western order. As traditional Western alliances evolve, BRICS faces the challenge of establishing itself as a viable alternative in international diplomacy.

## 5 Challenges and Opportunities for BRICS Peace Initiatives

While BRICS offers a counterbalance to Western-led institutions, internal policy differences, economic disparities, and regional security concerns present obstacles to unified action. The symposium concluded with reflections on how BRICS can strengthen its diplomatic coherence to become an effective peace-building force.

The International Conference on the Nexus between Security and Economy: BRICS Perspectives, held on 15 August 2024, marked a significant milestone in the ongoing dialogue about the intricate relationship between security and economic stability in the BRICS (expanded) nations – Brazil, Russia, India, China, and South Africa. This conference, which brought together leading scholars and practitioners, highlighted the importance of aligning security frameworks with economic priorities to foster sustainable development and resilience in an increasingly interconnected world.

The BRICS nations, with their diverse political, economic, and social landscapes, face unique challenges and opportunities. The conference highlighted how these countries, despite their differences, share common security threats – such as cybersecurity risks, energy insecurity, and socio-economic inequality – that have profound implications for their economic growth and stability. The discussions revealed that addressing these challenges requires not only national efforts but also regional and international cooperation.

One of the key takeaways from the conference was the recognition that *security and economic growth are deeply intertwined*. While robust security measures are essential for maintaining stability, overly restrictive policies can stifle economic activity by discouraging foreign investment and limiting trade. Conversely, economic instability which includes the challenge of youth unemployment in Africa but also further afield in the global South – can exacerbate security risks, creating a vicious cycle that undermines both national and regional progress. The conference emphasised the need for *strategic alignment* between security and economic policies, ensuring that they complement rather than conflict with each other.

Another critical theme was the role of *technology and innovation* in addressing security challenges and driving economic growth. Investments in cybersecurity, artificial intelligence, and renewable energy were identified as essential for mitigating risks and creating new economic opportunities. The conference also highlighted the importance of *socio-economic inclusivity,* particularly in countries like India and South Africa, where high levels of inequality contribute to social unrest and security risks. Addressing these disparities through education, healthcare, and job creation was seen as a prerequisite for achieving long-term employment opportunities, stability and prosperity.

The conference also shed light on the *geopolitical dimensions* of security and economic cooperation within the BRICS framework. As the global order continues to evolve, BRICS nations have the potential to play a pivotal role in shaping a more equitable and sustainable international system. However,

this will require a concerted effort to address internal challenges, such as political repression and human rights concerns, while fostering greater collabolaboration on shared security and economic priorities.

The insights and recommendations emerging from this conference are not only relevant for BRICS nations but also for the broader global community. In an era marked by rapid technological change, geopolitical uncertainty, and growing inequality, the need for integrated approaches to security and economic development has never been more urgent. The conference served as a timely reminder that *security and economy are two sides of the same coin*, and that addressing one without the other is unlikely to yield sustainable results.

As we move forward, it is imperative that BRICS nations continue to engage and upscale inter-, and transdisciplinary scholarship, research and dialogues, invest in innovation, and prioritise broad-based political, economic and social inclusivity in their policy frameworks. By doing so, they can not only enhance their own resilience and prosperity but also contribute to a more secure and equitable global order.

Drawing on the chapters and their abstracts, as usual, we provide a brief overview of select contributions at the 2018 symposium and the 2024 conference, and published in this special issue of *Alter*nation.

❋❋❋❋❋❋❋❋

## The 2018 BRICS PEACE & SECURITY SYMPOSIUM

The chapter by **Mosud Y. Olumoye and Stanley O. Ehiane, 'Cyber Terrorism and Cyber Security in Contemporary Nigeria',** seeks to explore the concepts of cyber terrorism and cyber security in an overview format. It is done in the context of the evolution and the accelerated development, adoption and use of Information and Communication Technology (ICT). ICT has transformed the modern world with both positive as well as negative impacts. Considering this fact, the one of the prevalent negatives, viz., cyber terrorism in Nigeria and its legislative response thereon. It covers topics such as elements of cyber terrorism; factors aiding cyber terrorism; techniques of attacks used by cyber terrorists; cyber terrorism in Nigeria; the impacts of cyber terrorism, and preventive measures for cyber terrorism. The chapter also addresses the effectiveness of cyber security to curb the threat of cyber terrorism. Methodologically, it is an explorative study that engages secondary data. The conclusion emphasises the

significance of effective cyber security strategies to maximise the benefits inherent in ICT for the growth and development of humanity.

**E.A. Mantzaris's** chapter, **'Corruption and Citizens' Financial Security in Public Service Medical Schemes: The Case of South Africa',** reports on an empirical exploration of public service medical schemes governance, its variations and the dire financial repercussions and financial security for the members of such schemes in South Africa. Given the class-based 'dual nature' of the medical scheme terrain in South Africa through the existence of 'open' and 'restricted' schemes (the latter dominated by public-service ones), existing violations of good governance take a wide variety of forms and types, despite the existence of legislation such as the Public Finance Management Act 1 of 1999 (PFMA), the Medical Schemes Act of 1998 and the regulatory body, the Council for Medical Schemes (CMS). Methodologically the research was based on a qualitative frame of research and included a scrutiny of primary and secondary documentary material as well as unstructured interviews with senior public service officials. In principle, the findigns are that beneficiaries of public services expect affordable, honest, accountable and useful services and products that are in accordance with their needs and financial means and resources. In terms of the duality of the market, such services ought to be delivered in a transparent, accountable and responsible manner, where accountability and common respect of the partners make this financial relationship sustainable. In this instance citizens utilize such products and services with the hope of a provision of a corrupt free service that is realistic and sustainable and guarantee financial security to citizens.

The prominent ambassador, **H.H.S. Viswanathan,** in his **'Can BRICS Contribute to Global Peace and Security?',** argues that peace and security is the sine qua non for progress and prosperity. History repeatedly shows that countries and regions prosper during periods of peace and stability. In BRICS (Brazil, Russia India, China and South Africa), as geo-economic entity, the increasing focus on geo-political peace and security has steadily grown in prominence over the last ten summit declarations. The question then arises as to whether the new emerging BRICS narrative from the Global South, can take a larger role in the maintenance of Global Peace and Security. It may do so, granted some seminal issues are addressed effectively, viz., i) BRICS is not a formal alliance; so how could the BRICS partners formulate and implement policies? ii) Given its geo-political diversity, BRICS countries may find common ground in Peacekeeping, Peace Building, anti-piracy, action against drug and human trafficking and anti-terror activities. iii) BRICS could also

address factors that lead to conflicts namely the non-traditional security threats like poverty, youth unemployment, non-inclusive growth, increasing disparity in the inequality gap, food and energy security. The creation of new global mechanisms and platforms and a new narrative may be vital for effectively dealing with these issues. Peace should be seen not only as absence of conflicts but also as absence of all factors that could lead to conflicts.

In **'The Menace of Cybercrime, Cyber Security and Regional Response: The Case of Africa', Isaac Luthuli,** explores the new untapped wealth of data and information mines, which is worth billions of dollars today. Focusing on cybercrimes or cyber-piracy the momentous digital revolution also experiences devastating attacks from cybercriminals. It is estimated that 'spending on cyber security will escalate from $86.4 billion in 2017 to $93 billion in 2018' (Cybersecurity Ventures 2017). Concomitantly, the chapter engages, i) the historical landscape on the need to enhance cyber security as countermeasure to cybercrimes and its evolving sophistication and complexity; ii) the usability and resourcefulness of the cyberspace as seminal to the digital revolution in all sectors of businesses, and irrespective of the dangers; iii) the trend of cybercrime and cybercriminals' activities globally and in especially regionally in Africa; as the spot focus; and citing examples from the main fast growing economic centres on the continent. As internet usage for banking, money transfers, ecommerce and social media usage are blossoming, and are augmented by mobile telephony, to address personal and data safety and protection from cyber-piracy or cybercriminals remains critical. This must be done via the appropriate cyberspace policy and legal measure innovation, with a need to do this in BRICS as well as globally.

The chapter, **'Brazil, South – South International Security Governance and Peace Operations (2003 – 2016)',** by **Kai Michael Kenkel** explores Brazil's recent contributions to South - South governance and a rethinking of cooperation between global Southern states, as they relate to issues related to international security. Humanitarian intervention – the use of military force to protect individual rights and uphold the principles underpinning the international system – stands as proxy in this instance for the country's participation in collective security measures and the provision of peace and stability at the global level. Brazil's contribution to a notion of security governance anchored in the Global South will be assessed through a focus on both material aspects – participation in United Nations-led peace operations (and non-participation in Western-led initiatives) – and ideational aspects such as debates on the norms governing intervention practice and those

regulating the practice of security governance in multilateral bodies. Here, the country's engagement with the 'responsibility to protect' is one example.

❋❋❋❋❋❋❋❋

## The 2024 BRICS SECURITY & ECONOMY NEXUSES CONFERENCE

**'The Use of the Internet for Nefarious Security Purposes: Policies, Developments and Challenges of Terrorist Content on Social Media',** by **W.J. Dayal & N.D. Gopal,** is a non-systematic desktop literature review that draws on publicly available sources and aims to provide recommendations to civil society, academic researchers, and policymakers tasked with combatting terrorist content on social media. It i) investigates the United Nations (UN) policy mechanisms by which members engage in counterterrorism and combatting terrorist narratives; ii) outlines the BRICS approach to combatting terrorism on social media through the lens of the last five (5) summit declarations, taken at the 10th to the 14th BRICS Summits from 2018 to 2022; iii) investigates terrorists' use of social media and the response from private companies to reduce terrorist content on their platforms; and iv) investigates how journalists and civil society are impacted by broad bans of terrorist content on social media by drawing on the case of an East African journalist. The research found that while the UN, BRICS and private companies combat terrorism through policy mechanisms and the development of technology, broadly banning terrorist content on social media can inadvertently intersect with journalists and civil society actors. The research recommends that restrictions on terrorist content on social media should offer protection to journalists and civil society who may share content without the intention to incite violence.

In his **'A Survey of Cybcersecurity Issues in BRICS Countries', Oluwafisayo Kaka,** assesses cybersecurity issues within BRICS countries and identifies policies and measures used to tackle identified cyberattacks. Global cybercrime mainly comprise of criminals stealing information, and using cyberspace for monetary gain, identity theft and to attack critical infrastructure. Since financial development with progressive financial growth of the BRICS countries are seminal for them, they are also targets for cybercrime. So, methodologically the study comprises of a systematic review of existing literature on the topic, that generated data from peer-reviewed journals,

government documents, reports, policy documents, and other relevant documents on the cybersecurity responses of BRICS countries. For countering cyberattacks, we need to know what these comprise of, what the existing policy and related technological responses and their implementation and evaluation are. The findings, are that some cybersecurity policies and regulations are dated; we have skill gaps in different organisations across governance, public and social sectors in society; and there is little cybersecurity collaboration between governments and private organisations in and between BRICS countries. Recommendations, including societal impact analysis and pointers towards future research are made.

The expansion of the BRICS adds to the diversity of economic and political systems amongst its members. **'Fostering Good Governance and Human Rights in an Expanded BRICS: Challenges and Opportunities',** by **Simbarashe Tembo** and **James Ndlovu** makes a contribution on this matter. With new and existing membership, ranging from liberal constitutional democracies to outright authoritarian regimes, the BRICS bloc will face a myriad of challenges in policy formulation and implementation. While diversity is often desirable, it is crucial for the bloc to establish normative principles for good governance, democracy and human rights and foster mutual respect and shared values among member states. They argue that as BRICS positions itself as an alternative to Western-led global institutions, a principle-based approach to its relations can bolster its moral authority in international affairs. A significant number of countries that have recently joined BRICS face significant challenges including repression, corruption and political and economic instability. They theorize that a shared commitment to human rights and good governance enhances economic development, peace and security, leading to more equitable and inclusive growth in member states. Relying on liberal theories of international relations and international law, the chapter firstly discusses the imperative for setting international human rights norms, tailored for context specific for BRICS countries, so as to enhance cooperation within the bloc. It then attempts to provide technical assistance by drawing from best practices to facilitate human rights-based cooperation and among member states. It argues that an expanded BRICS has potential to reinforce good governance, human rights and democracy.

In her, **'An Exploratory Study on the Transnational Illicit Drug Trade and its Dangers to BRICS Countries', Sandhya Maharaj** points out that drug addiction is a global scourge and is a threat to human survival. The United Nations in its World Drug Report (UNODC 2024a) states that almost

292 million people used drugs in 2022 – a 20% increase from 2012. This chapter examines the prevalence and impact of transnational illicit drug trafficking in the formidable political and economic alliance of BRICS. Methodologically, the study uses a scoping review that investigates the trade effects on public health, economic stability and social cohesion within BRICS jurisdictions, including how the inflow of illicit drugs is stopped. The production, trafficking, circulation and consumption of drugs like cocaine, heroin, methamphetamines, and synthetic opioids impacts public health, including the spread of HIV/ Aids, and both national and global security. Corruption, resource constraints, and complex international trafficking networks exacerbates the situation. The main requirement is the formation of a cohesive partnership of BRICS nations, together with a strong and strategic alliance with a co-ordinated anti-drug strategy. A unified BRICS response, spanning the four strategically located regions is vital in combatting the rising drug threat.

**Nontyatyambo Pearl Dastile's 'Cooperation in Countering Transnational Crime',** is a critical examination of the multifaceted domain of transnational crime, with a specific emphasis on strategies that hold promise for the mitigation and curtailment of such activities. The study delves into the exigencies of forming countering strategies for addressing the pervasive issue of transnational transgressions. Structurally, the discourse is partitioned into four chronological segments, initially focusing on contextualizing the ensuing argument through John Burton's theoretical prism. The author explores proposed multi-stakeholder interventions before culminating in prescriptive recommendations advocating for the BRICS nations to forge symbiotic alliances with academic institutions and other entities, thereby facilitating sustainable solutions to the pervasive issue of transnational crime.

South Africa's chronic and critically high rate of unemployment, particularly among youth, is cementing the country in a state of political, economic and social vulnerability. As one of the largest and most industrialised economies in Africa, it is perplexing that South Africa holds the highest level of youth unemployment in the continent. Notwithstanding South Africa's robust legal frameworks and sustained job-creation policy initiatives which arguably hold much promise for dealing with youth unemployment, our analysis suggests that efforts to date lack a holistic, consolidated approach to meaningfully resolving the issue of youth unemployment, the consequences of which threaten national and human security. In **'Youth Unemployment and the Threat to Peace and Security: The Case of South Africa', Shanya Reuben** and **Shaida Bobat** adopts a literature review methodological approach and presents a syn-

thesised narrative review on the current evidence and knowledge bases in the context of South Africa's youth unemployment. The overarching purpose of this literature review is to provide an overview of the multifaceted nature of youth unemployment in South Africa including the root cause, implications for national peace and security as well as an evaluation of the current strategies employed in tackling youth unemployment. Based on their analysis, they highlight the persistent challenge of South Africa's youth unemployment which pose significant political, economic and social threats to the nation. They provide some insights into potential pathways for dealing with South Africa's youth unemployment crisis, emphasizing in particular, a call for a unified, coordinated national strategy to maximise efforts in addressing youth unemployment.

The international community has experienced and witnessed a plethora of conflicts, violence, violent extremism, and wars, all leading threats to international peace and security. In **'Social Dialogue as a Vehicle to Address Peace and Security: An Analysis of the BRICS Formal Declarations' Nirmala Devi Gopal** and **Cresencia Nyathi** examines how BRICS have tackled global peace and security through formal declarations from Durban, Fortaleza, Ufa, Goa, Xiamen, Johannesburg, Brasilia, Moscow, New Delhi and Beijing, using a social dialogue approach. Throughout 2013 to 2022, these ten declarations indicate a transition from a focus on economic matters to encompassing broader social and political concerns. Using thematic analysis for content analysis, the findings suggest that the summits have expanded their focus from purely economic matters to encompassing social and political issues. It highlights the importance of a democratic UN Security Council, peaceful conflict resolution, cybersecurity, and international cooperation. It suggests the BRICS approach to peace and security should be enhanced through multilateral cooperation, gender integration, cybersecurity collaboration, conflict resolution, inclusive social dialogue, and global governance reforms.

The chapter by **Irina Yarygina** is titled, '**Institutional Investors in Russia: Security Problems and Prospects'**. The objective reasons for assessing the role of institutional investors as secure and valuable participants of the Russian financial market and forecast trends within the framework of various projects is explained by the necessity of optimizing their participation in serving the needs of national and international economy as well as using the tools of environmental policy promotion. The subject of the research is the activity of institutional investors in contemporary environment and possible ways of making them as secure financial intermediaries more effective in providing the

needs of the modern economy, especially in the fuel and energy complex as a key sector of the Russian Economy. The chapter provides a comparative analysis of the current set of factors and threats that affect the prospects of participation of institutional investors in financial markets. The complex analysis methodology, used in assessing the problems, involves considering the standpoint of the influence of a set of factors, subdivided into internal and external. Internal factors include the national market conditions and environmental issues. External factors reflect the long-term impact of a potentially adverse or favourable impact on the course of projects implement-tation, based on institutional investors' facility in spite of market turbulence or political sanctions.

Dating back thousands of years, India has traditionally been a maritime nation, owing to its expansive coastline of 7 500 kilometres. It also played a very significant role in its economy over millennia, and currently it includes and covers the Exclusive Economic Zone (EEZ) of nearly 2.7 million sq km. This EEZ contains a number of energy and natural resources, including oil, gas and coal. In **'India's Energy Security Vulnerabilities: Assessing Threats to Critical Offshore and Onshore Energy Infrastructure in the Indian Ocean'**, Gargi Sharma studies what India has categorised as Offshore Development Areas (ODAs) in its Exclusive Economic Zone to explore and exploit these resources for economic gains and a number of private as well as state owned companies have set up their installations in these ODAs for this purpose. On the one hand, the great waters serve as a gateway to prosperity in the form of trade and commerce opportunities, but on the other hand, they also pose a serious challenge to the peace and security of the country. In the context of this chapter, 'Energy Security Vulnerabilities' are defined as the susceptibilities and threats that compromise the stability, integrity, and safety of energy resources and infrastructure. These vulnerabilities encompass a range of non-traditional threats such as maritime terrorism, piracy and armed robbery which have been on the rise in the maritime space in the last few decades and can be attributed to the ignorance of littoral states as well as maritime law enforcement agencies towards maritime security (also known as 'sea blindness'). Perceiving maritime space as an extension of their theatre of operations, the illicit non-state actors such as maritime terrorists, pirates and armed robbers have been making good use of this sea blindness and targeting offshore assets including critical energy infrastructure as well as vessels for nefarious financial and political gains.

**Fagbemi Adebimpe Saheed** and **Nirmala Devi Gopal** present a review essay 'Form Global to National Views: Examining Intelligence

Gathering as an Intelligence-curbing Policy'. Pertinent to note is that insurgency has been a menace to the development of human capital and natural resources in globally. Every state is proffering solutions to curb the threat of insurgents' cum terrorists' groups mobilisation and activities. This chapter focuses on insurgency from the global, regional and national perspectives, in respect of three selected countries, Great Britain, Sri Lanka and France (globe), Kenya (Regional) and Nigeria (National). In addition, timely and accurate intelligence has been used by governments and security agencies to curb the activities of the insurgent groups. Yet the war against them still persist. The root causes of insurgency need to be addressed timely in order to curtail it. More so, some of the security agencies lack the required modern tools in gathering intelligence, such as measurement and signature intelligence (SIGMINT), signal intelligence (SIGINT), geospatial intelligence (GEOINT). The chapter concludes that insurgent groups operate differently based on their ideology, religion, political motivation, uneven distribution of resources, and secession. This requires in-depth study, with accurate, timely and prompt intelligence sharing between affected the governments and security agencies. It will so be able to combat and win the war against terrorists cum insurgent groups.

In **'Psychological Security: Exploring Community Engagement in Peacekeeping', Matshepo Matoane,** argues that psychological security is intertwined with peacekeeping, based on the feeling of security. Community engagement is a practice that is employed in peacekeeping to ensure security of communities. Adopting a qualitative case study approach and community psychology as a conceptual framework, this chapter seeks to understand how community engagement ensures the psychological security of communities. The chapter argues that psychological security within peacekeeping is dependent upon the conscious and active participation of communities for which security is required. The chapter further argues that representations of community and positions adopted in understanding this concept, have a bearing on how communities are engaged with. The study reveals that a subjective representation of community is associated with community empowerment, while an objective or value free representation of community is associated with a partially empowered community. Communities who feel empowered may be more likely to perceive psychological security in their environment.

The COVID-19 pandemic, caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), swiftly became a global crisis, prompting the World Health Organization (WHO) to declare it a pandemic in March 2020. Over the following two years, the virus evolved, leading to

numerous waves of infections and the emergence of the omicron variant by December 2021. The pandemic had profound impacts on healthcare, the economy, education, and public trust in 'science', the media and the authorities. In **'The Mistakes made in Response to the COVID-19 Pandemic: How to Deal with Future Pandemics', Gert Kruger** explores the governance mistakes made during the COVID-19 response and seeks ways to enhance future pandemic preparedness.

❋❋❋❋❋❋❋❋

This *Alter*nation African Scholarship Book volume #21 (2025), brings together some of the seminal chapters form the 2018 symposium and 2024 conference, and in fact extends the 2018 dialogue initiated at the symposium, and also captures seminal contributions at the 2024 conference. It brings together expert analyses and policy recommendations to assess and provide some pointers for BRICS' evolving role in global peace and security. As the world navigates complex geopolitical landscapes, the contributions in this volume provide a roadmap for BRICS to enhance its impact in conflict resolution, economic diplomacy, and cyber security governance.

The volume also captures the key themes, discussions, and recommendations from especially the conference, which serves as a valuable resource for policymakers, scholars, and practitioners seeking to navigate the complex interplay between security and economy.

It is our hope that the insights contained within these pages will inspire the further continuously developing BRICS dynamics, but also impact globally, in their inclusive and equitable multi-lateral research, collaboration, and collaborative action, so paving the way for a more secure and prosperous future for all.

**Acknowledgement**
The financial assistance of the National Institute for the Humanities and Social Sciences (NIHSS), towards this peer-reviewed research publication is hereby acknowledged. Opinions expressed, and findings, conclusions and recommendations arrived at, are those of the authors and are not necessarily to be attributed to the NIHSS.

Professor Nirmala Devi Gopal
Department of Criminology & Forensic Studies
Howard College Campus
University of KwaZulu-Natal
Durban, South Africa
Gopal@ukzn.ac.za

Professor Gert (H.G.) Kruger
Catalysis and Peptide Research Unit
University of KwaZulu-Natal
Durban, South Africa
Kruger@ukzn.ac.za

Dr. Sandhya Maharaj
School of Law
College of Law and Management Studies
University of KwaZulu-Natal, and
Attorney and Conveyancer of the High Court of South Africa
MaharajS2@ukzn.ac.za

# THE 2018
# BRICS
# PEACE & SECURITY
# SYMPOSIUM

# Chapter 2: Cyber Terrorism and Cyber Security in Contemporary Nigeria

**Mosud Y. Olumoye**
**ORCID iD: https://orcid.org/0000-0002-6584-6096**

**Stanley O. Ehiane**
**ORCID iD: https://orcid.org/0000-0001-6871-4526**

## Abstract

The evolution of Information and Communication Technology (ICT) has transformed the world into a global village. Today, the technological transformation has pervaded every facet of human endeavours. Ironically, the technology that was supposed to serve the needs of mankind, which of course they do serve, has suddenly become the biggest most prevalent threat. Africa and indeed Nigeria, have been caught up in the web of modernisation and the ICT revolution and have had their fair share of the benefits and the menaces of bridging the digital divide.

Considering the forgoing, this study seeks to explore the concepts of cyber terrorism and cyber security in an overview format. The study also highlights the cyber terrorism in Nigeria and its legislation thereon. The study also gives a snapshot into the elements of cyber terrorism; factors aiding cyber terrorism; techniques of attacks used by cyber terrorists; cyber terrorism in Nigeria; the impacts of cyber terrorism, and preventive measures for cyber terrorism. Lastly, the study addresses the effectiveness of cyber security to curb the threat of cyber terrorism. This is an explorative study with over-reliance on secondary data. The conclusion emphasises the significance of effective cyber security strategies to maximise the benefits inherent in ICT for the growth and development of mankind.

**Keywords:** Cyber-security, Cyber-terrorism, ICT, Nigeria

## 1 Background to the Study

The importance and roles played by Information and Communication Technology (ICT) and other auxiliary devices in organisations, institutions, government and our daily lives cannot be over-emphasised. Amongst the critical roles of ICT is the transformation of the whole world into a global village. The term ICT refers to a very versatile and powerful technology that is increasingly used as a strategic tool by people, organisations and nations to acquire, process, store and distribute information. Additionally, ICT has been identified as an indispensable tool to manage our daily lives and has become a necessity in our daily operations (Osho, Falaye & Shafi 2013). As the case may be, there has been a surge in the use of cyberspace in Nigeria, as the average citizens of the country use mobile phones while internet usage is steadily increasing.

However, the remarkable development in ICT skills and experience have created a new form of vulnerability popularly referred to as 'cyber terrorism' (Weimann 2004) which has been experienced and is still ongoing in both developed and developing nations of the world. Cyber terrorism has become a continuously evolving phenomenon with increasingly blurred boundaries in terms of definition. The development of ICT has meant that global development has suddenly become an instrument of destruction through the potential acquisition by terrorist groups. The terrorist groups such as the ISIS and Al Qaeda using cyberspace (Internet) have been able to conduct recruitments and propaganda radicalisation across the globe for network expansion and activities (Sinai 2016). The radicalisation and training of some Muslim Americans was conducted through the cyberspace (Internet) using social media like the Facebook. 'Nidal Hassan Abdul, a US army officer, [and] the radicalisation of Nigerian Omar Abdulmutallab, of British Airways were good examples' (Gabriela 2017:23). The terrorists, using various encryption technologies in operational functions, have been able to avoid the surveillance of the counter-terrorist advisories of the Americans and their European counterparts (Sinai 2017). In the past four decades, cyber terrorism has remained a catastrophic consequence for national security, due to sequences of synchronised attacks on the state's institutions and infrastructure such as the server of the CIA and British and Israeli security agencies (Gabriela 2017). The threat of cyber terrorism will be the biggest threat; this was the view of FBI Director Robert Mueller in 2012 (US Senate report 2014). The Senate report on the potential and imminent threat of cyber-attacks led to Barak Obama's administration's priority towards cyber security. The cyber-attacks have also

manifested in some countries like and Estonia (Gabriela 2017). In Iran a cyber-attack called 'Flame' hurt the Iran information system, and in May 2007 in Estonia two banks and the government IT infrastructure were paralysed (Gabriela 2017: 23).

Developing a cyber warfare capability requires personnel and technical knowledge, and it has been achieved through the recruitment of IT engineers and technicians by the terrorist groups. In certain situations, the terrorist groups contract the services of cyber attackers by paying mercenaries or state sponsors (Sinai 2016). This gives the terrorists the opportunity to launch an attack on any air traffic control and defence system. Also, it should be noted that the more advanced a country is technologically, the more its infrastructure becomes susceptible to cyber-attacks.

Presently, there is an unabated growth in the threat of cyber-attacks in Africa and with the evolution of cybercrime it has led to more uncontrollable and sophisticated attacks. In Africa cyber-attacks have left the government institutions and the banks most vulnerable due to the lack of independent ICT infrastructures, budgetary challenges, poorly trained staff, and a lack of and weak implementation of legislation. African countries struggle to address cybercrime despite the popular Pan African Legal (PAL) document in the convention of the African Union on Cybersecurity and Protection of Personal Data (AUCPPD). Nigeria is ranked among the worst nations regarding the abuse of ICT (Internet Crime Complaint Centre 2010); where terrorists, hackers and other forms of criminals and their agents use it as a tool to perpetrate their unlawful acts. It should be noted that a county with weak cyber security is potentially vulnerable to cyber terrorism, where terrorist groups operate. Consequently, this study basically explores the concept of cyber terrorism and cyber security. Also addressed in the study are the elements of cyber terrorism; factors aiding cyber terrorism; techniques of attacks used by cyber terrorist; cyber terrorism in Nigeria; impacts of cyber terrorism and preventive measures for counter attacks.

## 2 Concepts of Cyber Terrorism and Cyber Security

### *2.1 Cyber Terrorism*

The term terrorism has been in existence since the 18$^{th}$ century prior to the incidence of the French revolution (Nadjib 2017). However, the act became well known after the September 11 2001 attack on the World Trade Centre in the United States. Hence, the US President, George Bush, declared war against the

terrorists across the globe. Responding to the declaration made by the US, the Al-Qaeda led terrorist group determined to challenge not only the Western countries which are considered to be their enemies; but other nations of the world such as Indonesia, Libya, Pakistan, and considered to have deviated from pure Islamic ideology (Nadjib 2017). Cyber terrorism according to Colarik (2006:46), is the 'premeditated, politically motivated attacks by subnational groups or clandestine agents, or individuals against information and computer systems, computer programs and data that result in violence against non-combatant targets'. This definition differentiates cyber terrorism from cyber-crime[1] and cyber warfare[2]. The whole excess of cyber terrorism is to induce fear and harm as a resort of political inclination. Colarik's proposition juxtaposes Abolurin's (2011:24) definition of cyber terrorism as the 'application of information technology to attack non-combatant and attract attention to their cause'. The whole idea of fear in this context is considered as violence and this has physical consequences as it portrays the purpose of the attackers (Janczewski & Colarik 2008:14). Imagine if a person gains access to an institution's clinical database and changes the patients' medication and a duty nurse comes in to administer the medication and discovers that the patients die after dispensing the medication. If the initiator threatens to commit more acts of this nature if his demands are not met, this is referred to as cyber terrorism. The context is based on the intention that drove the perpetrator's action and the use of information technology to perpetrate the act and not the action.

Furthermore, terrorism has become a global threat to all nations of the world encompassing lives and properties, government, economic and social realms. Contrary to the conventional terrorism which employs kinetic means such as the improvised explosive devices (IEDs) or suicide bombers (Gross, Canetti & Vashdi 2017) to accomplish their missions, the cyber terrorists employ ICT to advance their religious, ideological and political goals to psychologically and physically hurt the people, more especially the civilians. Cyber war and cyber-crime differ from the cyber terrorism under study. Cyber war connotes the use of viruses and malware to deactivate military setups (Canetti & Vashdi 2017); while cybercrime targets pecuniary benefits to make

[1] Cyber-crime is frequently used by law enforcement agencies and is an offence committed using information technology (Janczewski & Colarik 2008:14).

[2] Cyber warfare is a planned attack by nations or their agents against information and computer systems, computer programmes, and data which result in enemy losses (Janczewski & Colarik 2008:14).

a living, create criminal mischief or for personal pleasure (Olumoye 2011). Moreover, in this era of continued increases in cyber-attacks and terrorist activities, the fear of cyber terrorism has become prevalent and has come to stay. The term 'cyber terrorism' was first coined by Barny Collin in 1982 and was consistent with how the physical and cyber world were merged in relation to some aspects of terrorism (FBI 2011; Riglietti 2016). Cyber terrorism is not only a change from the conventional to a more modern terrorism, but a reflection of a technologically advanced and literate generation using high technology tools with all their sophisticated features such as speed, accuracy, mobility and connection to attack the cyberspace (Nadjib & Cangara 2017).

Thereafter, various scholars in ICT and other fields of study came up with different definitions for cyber terrorism based on their experiences and views. Hence, different definitions have been attributed to cyber terrorism. However, this study adopts one of the most popular and cited definitions of cyber terrorism given by Professor Denning which states that cyber terrorism is a deliberate action taken against the computer system (hardware and software), networks and the information stored there in order to disrupt, degrade, deny access to or destroy (Denning & Denning 2010). Cyber terrorists use a computer network to pose harm to human life or destroy the important and national infrastructure in a way that will affect the citizens and paralyse the nation's economy (Kuboye & Osman 2014). This study aligns with the focus of Bogdanoski and Petreski (2013) that states that if drastic measures are not taken to tackle the increase in cyber terrorism, then the future terrorists will emerge in any of their attacks to destroy the infrastructure that depends largely on ICT without necessarily firing a shot.

### *2.1.1 Elements of Cyber Terrorism*

Several cyber terrorism attacks that have taken place have some fundamental elements which have been identified by researchers in the academic community. According to Denning's (1999) definition, the elements required for cyber terrorism include: the partakers are non-state accomplices; attacks are basically computer-based with damages done on IT based installations; victims of attacks are either for social, religious or political reasons; a cyber terrorism attack is done only within cyberspace (Nadjib & Cangara 2017). In addition, other scholars identified five entities that make up cyber terrorism namely: target of the attacks; mission and reason (motivation) behind the attack; tools to launch the attack; domain to carry out the attack; and the impact of such attacks

(Ahmad, Yunos & Sahib 2012). Mackinnon *et al*. (2013) in their study state that most of the contemporary definitions on cyber terrorism only identify three elements, the terrorists' motivation; the cyber system under target and the impact of the attacks. This study discusses these elements of cyber terrorism in order to have a better understanding of the concept and to identify the profile of actions motivating the perpetrators.

### *2.1.2 Factors Aiding Cyber Terrorism*

One of the critical factors aiding cyber terrorists is the anonymous nature offered by the internet which allows the identity of the evil perpetrators to be hidden. This supports Awan (2014) who states that the terrorists use the internet because it is a safe environment and a hidden platform for them to perpetrate their atrocities since their identities remain anonymous and they need not travel far to launch an attack. Moreover, the terrorists use fake identities during operations which are untraceable.

Another facilitating factor is the supportive nature of the internet. The internet is also referred to as an information super-highway because it connects several thousands of different networks from more than two hundred countries across the globe together (Olumoye 2011). The cyber terrorists use the internet because of this connectivity (supportive) characteristic in order to send messages to millions of people across the globe. According to Awan (2014), the terrorists use the platform to recruit interested people globally.

### *2.1.3 Techniques of Attacks Used by Cyber Terrorists*

There are different techniques adopted by terrorists to unleash their attacks on ICT infrastructures. This was buttressed by Bogdanoski and Petreski (2013) who state that cyber terrorists carry out attacks in different ways. Some of these techniques are discussed accordingly.

#### Hacking

Hacking generally refers to the act of gaining unauthorised access to a computer, networks, websites or areas of a system (Olumoye 2013). According to Moffitt *el al.* (2012), hacking is the unauthorised access into or interference with a computer system, or any access in order to corrupt, alert, stall or destroy information using a computer or other similar information and communication

devices, without the knowledge and consent of the owner of the computer or information and communication system. This includes the introduction of computer viruses and the likes resulting in the corruption, destruction, alteration, theft, loss of electronic data messages or electronic document. Many of the hackers use 'brute force' which involves combining different letters and numbers until they can get the password that can be used to launch their devilish attack.

## Eavesdropping

This method involves the use of software (password sniffers) to monitor packets, or wiretapping telecommunication links to read transmitted data. Eavesdropping can go undetected and it is called a passive attack (Olumoye 2013). Tools used to intercept communications can be cellular, scanners, radio receivers, microphone receivers, tape recorders, network sniffers and telephone tapping devices (Ibikunle 2005). This method is usually used for monitoring all the traffic in on an area network, which the terrorists install on the network system they plot to intrude, such as the ICT-based installations and telephone systems (Hassan, Funmi & Makinde 2012).

## Malware

Malware refers to malicious software such as viruses, Trojan worms and other software that gets onto a computer without the owner being aware it is there. Back in the early part of the century, most of such software's primary aim was for excitement (Olumoye 2013). The people writing the software found it amusing to write a program that exploited security flaws just to see how far it could spread. Today the incentive for developing such software is generally more sinister and that is the reason it makes the list of the top five computer crimes (Anonymous 2012). Cyber weapons are now identified as the main software tools used by cyber terrorists to wreak havoc on any country and organisation in order for them to accomplish their mission such as manipulating computers and their networks, intrusion into systems, and sending spy (espionage) mails in the form of viruses.

## Spam Messages

Spam refers to the release of unsolicited bulk messages. The cyber terrorists use spam messages as a tactic to launch their attacks**.** Though the attackers use

numerous forms of spam messages, the most frequently used ones are spam e-mails which can be disguised in the form of an advertisement for goods and services (Kuboye & Osman 2014). Once the recipient opens the mail, the password as well as the username are generated automatically which can later be used to intrude their mails and launch attacks (Gercke 2012).

### *2.2 Cyber Security*

Defining cyber security at large is not trivial. The difficulty lies in developing a definition that is broad enough to be valid regardless of the system that is being described, yet specific enough to describe what security is (Olumoye 2013b). However, in a generic sense, security is 'freedom from risk or danger'. According to Laudon and Laudon, cyber or information system security can be described as 'the policies, procedures and technical measures used to prevent unauthorised access, alteration, theft, and physical damage to information system' (Laudon & Laudon 2001: 13). Cyber security, which is otherwise referred to as a preventive measure, is an offensive technique to combat cyber terrorism (Osho, Falaye & Shafi 2013). Whatever security method that may be adopted there is a need to ensure that only authorised users can access the organisation's information system, and that the users only perform the job and view the data they are authorised to access (Olumoye 2011). Securing the cyberspace is more important than ever before, just as the physical space is to the survival of mankind, which simply means that the security of the cyberspace is not only essential to prevent cyber-attacks but becomes indispensable to prevent other forms of attacks that can be done through the cyberspace (Osho, Falaye & Shafi 2013). Thus, cyber security turns out to be an intelligent tool for counter terrorism.

## 3 Cyber Terrorism in Nigeria and State Response

### *3.1 Terrorism*

Terrorism is usually a direct consequence of the peoples' profound disappointment with government. The maltreatment or mismanagement of the critical issues have led to the emergence of various rebellious groups across the Nigeria geographical areas. These include the Bakassi Boys in the South-South; the Oodua People's congress (OPC) in South-West; The Movement for the Actualisation of the Sovereign State of Biafra and Independence People of Biafra (IPOB) in the South-East; the Movement for the Emancipation of the

Niger Delta (MEND) in the South-South; and the *Jama' Ahlus Sunnah Lid Da'awati Wal Jihad*, also known as Boko Haram in the North-East. The major actions of these groups have been perceived as a retaliation to the incapability of the government or society to meet their demands. According to Osho, Falaye and Shafi (2013), cyber terrorism trends in Nigeria have been enthused from the grievances motivated from mainly religious fundamentalism to socio-economic reasons. Without any doubt, cyber terrorism is still in its infancy stage in Nigeria and is being perpetuated by a small portion of the total populace; invariably, a small percentage of the nation's cyber space users. This was substantiated by Osho, Falaye and Shafi (2013) that the activities of terrorists in Nigeria are still mostly traditional in nature. For instance, the attack of some telecommunication masts (MTN and Airtel) were recorded in Bauchi, Borno, Kano, and Yobe State (Adeyemo, Joel & Tsenzhughul 2012). The terrorist attack on the telecommunication masts was mainly to limit the use of mobile technology in order to prevent communication of messages to the public and access to the internet. Moreover, before the 1st October 2010 Abuja bombing, the MEND revealed their strategies to the security agencies using the internet technology (Jeremy 2010). In a recent development, the terrorists have adopted another dimension of cyber terrorism. In this case, politicians, foreigners and people assumed to be rich are kidnapped, while the relatives or government representatives are contacted through phone calls. Intelligence reports have also revealed that Boko Haram has linked up with Al-Qaeda based in Algeria (*The Nation Newspaper* 2011). This implies that Boko Haram may be equally trained on the use of ICT to advance their operations and attacks.

## *3.2 Nigerian Government Legislation in Fighting Cybercrime: The Nigeria Cybercrime Act 2013*

The objectives of this Act are to,

(a) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;
(b) ensure the protection of critical national information infrastructure; and
(c) promote cyber security and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.

The application of this Act shall apply throughout the Federal Republic of Nigeria.

The Act prevent for Cyber terrorism and provides that any person who accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable to conviction of life imprisonment. The Act further provides for the purposes of this section, 'terrorism' shall have the same meaning under the Terrorism (Prevention) Act 2011, as amended. The Nigerian legislation on Cybercrimes Act 2013 clearly provides for cyber terrorism and the Act is an offshoot of the Council of Europe Convention Cybercrime and ECOWAS Directive on Fighting Cybercrime. The realisation of this Act by the Nigerian Government has addressed the complexity in Article 22 of the Council of Europe on the issue of nationality, territoriality and jurisdiction. The offences in the Convention, ECOWAS Directive all encompasses an established criminal law model for all the nations (The Nigerian legislation on Cybercrimes Act 2013).

## 4 Impacts of Cyber Terrorism

Cyber terrorism which is still advancing in Nigeria has many potential impacts when it is launched either against the organisations or nations. Some of the impacts of cyber terrorism are discussed accordingly.

### *4.1 Attacks on Computer-based Infrastructure*

The advancement of any organisation or nation is dependent on the critical infrastructure upon which their work is carried out and the exchange of vital information. It becomes apparent that any attack launched on a nation's infrastructure would paralyse its economy. This is corroborated by Thuraisingham (2004) who states that cyber-attacks can be launched on any infrastructure such as the electronic, gas, power, telecommunication lines, food supplies, reservoirs and water supplies, and other vital things; which can lead to the total shut down of an organisation.

### *4.2 Attack on Businesses*

Cyber terrorism has a tremendous impact on society. The impact of a single attack can be very devastating and culminate in huge financial losses. The overall monetary impact of cyber terrorism on individuals and government runs

into billions of dollars (Olumoye 2013). Also, there is a food chain effect when society finds out an organisation is vulnerable to cyber terrorism. Firstly, the company is made aware of their weaknesses. Customers and companies could potentially lose personal information that could then be sold for a profit. The company then loses credibility and profits begin to fall. Secondly, if the market falls, then demand decreases which reduces supply and demand, potentially shutting down a company or sending them into bankruptcy (Muffitt *et al*. 2010). Moreover, customers' trust is affected as the attack of terrorists may intrude into other cyberspace areas thereby discouraging and frustrating the customers or end users who usually visit the concerned page for their business dealings (Saini, Rao & Panda 2012).

### *4.3 Aggravation, Personal Insecurity and Loss of Life*

According to Gross, Canetti and Vashdi (2017), cyber terrorism impacts on civilians by aggravating personal insecurity and anxiety. Moreover, cyber terrorism has rendered many homes to a dilemma which sometimes results in psychological trauma to the family's victims. This has also claimed many innocent lives. In support of this, Awan (2014) states that cyber terrorism can cause serious damages or loss of life, some of which has manifested in a number of ways through the attack of networks and computer usage resulting in different forms of explosions experienced by planes globally and culminating in the loss of many lives.

### *4.4 Intrusion into Data*

It is apparent that processed data (or information) is required to perform numerous functions within an organisation. The intrusion or attack of a nation or organisation's information by cyber terrorists can lead to the loss of vital and critical information which may be difficult to recover. This view was strengthened by Koltuksuz (2013) who states that cyber terrorists can interrupt data availability and destroy its confidentiality as well as integrity.

## 5 Preventive Measures against Cyber Terrorism

In order to prevent the attacks of cyber terrorists in our society, the following preventative measures are recommended.

### *(i) Awareness and Training*

This is the first set in alleviating cyber terrorism. The citizens, consumers and organisations should create the awareness of cyber threats and the actions they can take to protect their information. Also, continuous training is necessary for business clients in order to share the responsibility in fighting against cyber terrorism (Olumoye 2013b).

### *(ii) Ethical and Moral Standards*

Ethical standards should be upheld in organisations to ensure that confidentiality is maintained, and technology misuses are reduced. Computer ethics help us to identify offenders and create solutions to aid in the minimisation of computer crimes and technology misuse (Moor 1985; Olumoye 2013b).

### *(iii) Computer Forensics*

Computer forensics technically refer to the use of procedure-centric approaches in the study of cyber-attack prevention, planning, detection and responses with the goals of counteracting and conquering hacker attacks by logging malicious activity and gathering court admissible chains of evidence using various forensics tools that reconstruct criminally liable actions at the physical and logical levels (Mandia *et al.* 2001; O'Connor 2003). According to Ibikunle (2005), an advanced computer forensics is the use of steganography, which is the art of hiding communications. Unlike encryption that uses an algorithm and a seed value to scramble or encode a message to make it unreadable; steganography makes the communication invisible. This takes concealment to the next level, which is to deny that the message even exists (Olumoye 2013b).

### *(iv) Cyber Crime Prevention Laws*

According to Mc Connell (2000), National government remains the dominant authority for regulating criminal behaviour in most places in the world. If a nation has already struggled with and ultimately improved its legal authority after a confrontation with the unique challenge presented by cybercrime; it is crucial that other nations profit from this lesson and examine their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cyber criminals. In many cases, nations

will find that current laws ought to be updated. Enactment of enforceable computer crime laws that also respect the rights of individuals are an essential next step in the battle against this emerging threat (McConnell 2000). The attackers' sophistication seems to be ahead of defensive tools. That is the nature of the war between hacker and defenders; the attackers are always a step ahead. However, by making the attackers' job harder and harder, and by increasing the length of jail sentences for cybercrime and improving international police co-operation and skill levels, defenders can combine to keep up with the attackers and over time begin to turn the tide (Paller *et al.* 2007).

### *(v) Encryption (or Cryptography)*

This involves scrambling data into an unreadable format called cipher text before it is transmitted over a telecommunication link between two computers, and then unscrambling that data again when it gets to its destination computer. Only those who possess the secret key can decipher (or decrypt) the message into plain text. If data is not encrypted during transmission, it can easily be intercepted by an unauthorised party thereby enabling the third party to have access to the information. Encrypted messages can sometimes be broken by cryptanalysis, also called code-breaking; although modern cryptography techniques are virtually unbreakable (Olumoye 2013b). Cryptography is used to protect e-mail messages, credit card information and corporate data.

### *(vi) Anti-Virus*

Anti-virus is a software program that is used to protect computer systems against the menace of viruses. The effect of this software is to detect and remove a virus from a computer system before it does any damage to it. These software programs can readily be purchased from software stores or downloaded from the internet. Examples of antivirus software are: Shield Deluxe, CA anti-virus, BitDefender, Avira, Kaspersky, Avast, Norton, NOD32, Dr. Solomon, MCAFFEE, MSAV and AVG (Olumoye 2013b).

.

### *(vii) Firewall*

Firewalls are made up of software and hardware placed between an organisation's internal and external networks to prevent outsiders from invading their networks. Firewalls are programmed to intercept and examine any

message packet passing between the two networks and reject unauthorised messages (Olumoye 2013b).

### *(viii) Passwords*

Passwords are a unique set of characters that may be allocated to an individual, a system or facility that must be input to allow access. Passwords are a security measure used by computer users which allows only authorised users to gain access to the system. The lack of a password on a computer system increases the risk of unauthorised access. To prevent hackers and crackers from penetrating a network, it is recommended that one use passwords that are difficult to guess. It is better to make the password a mixture of letters, numbers and special characters such as: @! $, %, ‘, &, *, # etc. Moreover, one should always change one’s passwords at regular intervals and also set a minimal length for the passwords such as a minimum of six or eight characters (Olumoye 2011).

## Concluding Remarks

This manuscript was commenced bearing in mind that the current threat of cyber terrorism seems not to be noticeable and has recently virtualised in Africa, particularly Nigeria, where the terrorist group called Boko Haram have gained their stronghold. In the United States, Europe and the Middle East cyber terrorism remains an existential threat to the critical infrastructures, and steps are being taken through the application of cyber security to safeguard the country’s facilities. The invisible nature of cyber terrorism allows ample and considerable time for the perpetrators to escalate the lethality of their warfare in a more convergent manner. The African continent, particularly Nigeria, needs to understand the various nomenclatures regarding cyber terrorism in the wake of the ongoing traditional terrorist attacks. In light of the foregone, this study contextualised cyber terrorism and cyber security as two sides of the coin in terms of threat and protection. The study further examined factors aiding cyber terrorism and techniques used to unleash the menace across the globe, along with the potential and physical impacts. This study serves as an early warning to Africa and Nigeria in particular, because West Africa has become a ‘safe haven’ for Boko Haram now branded the Islamic State of West Africa Province (ISWAP). However, beyond the Cybercrime Act of 2013 enacted by the Nigerian government to protect the cyberspace and the potential impacts of

cyber terrorism capable of crippling the nation's infrastructure, the government should address the current challenges of cyber security in the country. The protection of cyberspace will prevent the terrorist group from winning the asymmetric war without the use of arms and ammunitions.

## References

Abolurin, A. 2011. *Terrorism: Nigerian and Global Dimensions.* Nigeria: Golden Gems Unique Multiventures Publishers.

Adeyemi, K., D. Joel & A. Tsenzughul, September 2012. Gunmen Attack MTN, Airtel Masts in Kano, Borno, Bauchi, Yobe. *The Nation Newspaper.* Available at: http://www.thenationonlineng.net/2011/news/60494-gunmen-attack-mtn-airtel-masts-in-kano-borno-bauchi-yobe.html (Accessed on 06 September 2019.)

Ahmad, R., Z. Yunos & S. Sahib 2012. Understanding Cyber Terrorism: The Grounded Theory Method Applied. In Cyber Security, Cyber Warfare and Digital Forensic CyberSec 2012 International Conference. *IEEE and American Foreign Policy Decision Making*. San Francisco: The World Affairs Council. Available at: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf (Accessed on 28 July 2016.) https://doi.org/10.1109/CyberSec.2012.6246081

Anonymous 2012. *Top Five Computer Crimes and How to Protect Yourself from Them*. Available at: http://www.makeuseof.com/tag/top-five-computer-crimeprotect (Accessed on 17 August 2012.)

Awan, I. 2014. Debating the Meaning of Cyber Terrorism: Issues and Problems. *Internet Journal of Criminology* 1 - 14.

Bogdanoski, M. & D. Petreski 2013. Cyber Terrorism – Global Security Threat. *Contemporary Macedonian Defense – International Scientific Defense, Security and Peace Journal* 1324: 59 - 73.

Colarik, A.M. 2006. *Cyber Terrorism: Political and Economic Implications.* London: Idea Group Publishing. https://doi.org/10.4018/978-1-59904-021-9

Denning, D. [1999] 2001. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In Arquilla, J. & D.

Ronfeldt (eds.): *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND Corporation.

Denning, P.J. & D.E. Denning 2010. Discussing Cyber-attack. *Communications of the ACM* 539: 29 – 31. https://doi.org/10.1145/1810891.1810904

Gabriela, S.L., March 2017. Manifestations of Contemporary Terrorism: Cyberterrorism. *Research and Science Today* 1,13. Available at: https://www.rstjournal.com/wp-content/uploads/2017/03/RST-1-2017.pdf (Accessed on 30 September 2019.)

Gercke, M. 2012. Understanding Cybercrime: Phenomena, Challenges and Legal Response. ITU, UNESCO.

Gross, M.L., D. Canetti & D.R. Vashdi 2017. Cyber Terrorism: Its Effects on Psychological Well-being, Public Confidence and Political Attitudes. *Journal of Cyber Security* 3: 49 - 58. https://doi.org/10.1093/cybsec/tyw018

Hassan, A.B., D.L. Funmi & J. Makinde 2012. Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology* 27.

Ibikunle, A. 2005. *Investigation of Computer Crime in the Information Technology Industry*. Unpublished Master's dissertation, Ladoke Akintola University of Technology.

Internet Crime Complaint Center 2010. Internet Crime Report. Available at: www.ic3.gov/media/annualreport/2010_ic3report.pdf (Accessed on 04 September 2019.)

Jenczewski, L. & A.M. Colarik 2008. *Cyber Warfare and Cyber Terrorism*. USA: IGI Global. https://doi.org/10.4018/978-1-59140-991-5 PMid:17605410

Jeremy, W. 2010. Nigeria Explosion: Independence Celebrations Marred by Violence. Available at: http://www.csmonitor.com/World/Africa/Africa-Monitor/2010/1001/Nigeria-explosion-Independence-celebrations-marred-by-violence (Accessed on 30 September 2019.)

Koltuksuz, A. 2013. Use of Cyberspace and Technology by Terrorists. *Technological Dimensions of Defence against Terrorism* 115: 106. https://doi.org/10.3233/978-1-61499-317-9-106

Kuboye, O.S. & W.R.S. Osman 2014. Cyber Terrorism Attack of the Contemporary Information Technology Age: Issues, Consequences and Panacea. *International Journal of Computer Science and Mobile Computing* 35: 1082 - 1090.

Laudon, K.C. & J.P. Laudon 2001. *Essentials of Management Information Systems*. New Jersey: Prentice Hall.

MacKinnon, L., L. Bacon, D. Gan, G. Loukas, D. Chadwick & D. Frangiskatos 2013. Cyber Security Countermeasures to Combat Cyber Terrorism. In Akhgar, B. & S. Yates (eds.): *Strategic Intelligence Management: National Security Imperatives and Information and Communication Technologies.* London: Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-407191-9.00020-X

McConnell 2000. *Cyber Crime … and Punishment? Archaic Laws Threaten Global Information*. McConnell International. Available at: http://www.mcconnellinternational.com/services/cybercrime.htm (Accessed on 08 August 2005.)

Moffitt, T., C. Pannatia, B. Prosenbeck, E. Scott & D. Siversen 2012. *The HRE Online Experience - Technology Misuse and Cyber Crime*. Available at: https://sites.google.com/site/tommoffittportfolio/the-hre-online-experience/technologymisuse-and-cyber-crime (Accessed on 20 October 2013.)

Nadjib, M. & H. Cangara 2017. Cyber Terrorism Handling in Indonesia. *The Business and Management Review* 92: 274 - 283.

O' Connor, T., March 2003. *Glee, Elation and Glory as Motives for Cyber Crime*. Annual Meeting of the Southern Criminal Justice Association. Nashville. Available at: http://faculty.ncwc.edu/toconnor/gleeelation_glory.htm (Accessed on 15 August 2005.)

Olumoye, M.Y. 2011. *Information and Communication Technology and Data Processing*. Lagos, Nigeria: Heralds of Hope Publishers.

Olumoye, M.Y. 2013. Cyber-crime and Technology Misuse: Overview, Impacts and Preventive Measures. *European Journal of Computer Science and Information Technology* 13,3: 10 - 20.

Osho, O., A.A. Falaye, A.A. & M.A. Shafi 2013. Combatting Terrorism with Cyber Security: The Nigerian Perspective. *World Journal of Computer Application and Technology* 14: 103 - 109. https://doi.org/10.13189/wjcat.2013.010401

Riglietti, G. 2016. Defining the Threat: What Cyber Terrorism Means Today and What it Could Mean Tomorrow. *The Business and Management Review* 83: 12 - 19.

Saini, H., Y.S. Rao, Y.S. & T.C. Panda 2012. Cyber-crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications (IJERA*) 22: 202 - 209.

Sinai, J. 2016. Threat Convergence: A New and More Lethal Category of Terrorist Warfare. *The Journal of Counter Terrorism* 223.

*The Nation Newspaper*, 16 November 2011. Boko Haram has Links with al-Qaeda – Algerian Minister. Available at: http://www.thenationonlineng.net/2011/index.php/news-update/26240-boko-haram-has-links-with-al-qaeda-algerian-minister.html (Accessed on 18 September 2019.)

The Nigerian Legislation on Cybercrimes Act 2013.

Thuraisingham, B. 2004. Data Mining for Counter-terrorism. *Data Mining: Next Generation Challenges and Future Directions* 157 - 183.

Weimann, G. 2004. Cyberterrorism: How Real is the Threat? United Nations Institute of Peace: Special Report. https://www.usip.org/sites/default/files/sr119.pdf (Accessed on 20 September 2019.)

Mosud Y. Olumoye
Webster University
George Herbert Walker School of Business & Technology
St. Louis, Missouri
USA
myolumoye@yahoo.com
yinusamosud@webster.edu

Stanley O. Ehiane
University of Botswana
Department of Political Science and Administrative Studies
Gaborone
Botswana
stanleyehiane@yahoo.com
ehianes@ub.ac.bw

# Chapter 3: Corruption and Citizens' Financial Security in Public Service Medical Schemes: The Case of South Africa

**E.A. Mantzaris**
**ORCID iD: https://orcid.org/0000-0003-0490-6953**

## Abstract

The article reports on an empirical exploration of public service medical schemes governance, its variations and the dire financial repercussions and financial security for the members of such schemes in South Africa. Given the class-based 'dual nature' of the medical scheme terrain in South Africa through the existence of 'open' and 'restricted' schemes (the latter dominated by public-service ones), existing violations of good governance take a wide variety of forms and types, despite the existence of legislation such as the Public Finance Management Act 1 of 1999 (PFMA), the Medical Schemes Act of 1998 and the regulatory body, the Council for Medical Schemes (CMS).

It is understandable that the beneficiaries of public services of this nature expect them to provide affordable, honest, accountable and useful services and products that are in accordance with their needs and financial means and resources. In this case the beneficiaries are able to guarantee their financial security, appropriate and accurate free credit reports that allow them to make decisions that are in accordance with their financial needs.

In such a situation and given the duality of the market, such services ought to be delivered in a transparent, accountable and responsible manner, where accountability and common respect of the partners makes this financial relationship sustainable. In this instance citizens utilize such products and services with the hope of a provision of a corrupt free service that is realistic and sustainable, and guarantee financial security to citizens.

The research was based on the qualitative frame of reference and included a scrutiny of primary and secondary documentary material as well as unstructured interviews with senior public service officials.

**Keywords:** Corruption, medical schemes, 'open' and 'restricted' medical schemes, GEMS

## Introduction and Context

Medical schemes violation of good governance associated with fraud and corruption is one of the many facets of health care corruption, avarice and greed, whether individual or collective. Like all healthcare fraud and corruption, this is an ever-growing 'industry', taking advantage of systemic, organizational and administrative weaknesses and challenges facing this multi-billion industry. Such corruption takes a variety of types and forms both nationally and internationally, such as falsification of patient data; referrals to specific medical service providers or/and suppliers; provision of false invoices; collusion between patients and medical scheme staff; kickbacks operations; misrepresentation of diagnoses; miscoding or misquoting of claims, and collusion (Salter 2010; Russell 2015; Whistleblowers International 2016; United Nations 2017).

Healthcare fraud directly impacts the quality and cost of care that a patient receives, and can put patients' lives at risk when they are exposed to treatment or procedures that are not medically warranted. Since medical aid fraud and corruption takes a wide variety of forms, detection, investigation, monitoring and prevention are not easy. This reality is exacerbated by the fragmentation and lack of coordination amongst medical aid schemes and the lack of consolidation, especially amongst the 'restricted' ones. The non-existence of a 'central data-base' in the sector in fact helps fraud and corruption at all levels, as collective coordination is lacking.

## The Medical Scheme Terrain in South Africa

There are 82 existing medical aid schemes in South Africa. They are governed by the Medical Schemes Act of 1998 and are regulated by the Council for Medical Schemes (CMS), a well- respected body that in 2017 received an unqualified audit report from the Auditor General of South Africa), for a record 17th time in a row (Auditor General 2017). This is an achievement unparalleled in the history of South African regulators and state institutions in their attempts to manage their financial affairs and comply with the dictates of the Public Finance Management Act 1 of 1999 (PFMA).

CMS has structured the regulatory processes of duties, responsibilities and obligations of the schemes such as compliance enforcement, administrative

accreditation, management of healthcare organisations and brokers, and investigations for all role players in the industry (both service providers and beneficiaries), according to the dictates of the Medical Schemes Act.

The 82 medical scheme entities comprise 22 'open' and 60 'restricted' schemes with 8.879 million members as at 31 December 2016, a small increase of 0.78% in comparison with the previous year and 8.814 million in 2014. Because of the significance of the Council of Medical Schemes and its role in the sector and society at large, it is deemed important to briefly deal with the key fundamentals facing the medical schemes in the country, based on the official documents of the regulator for the last financial year (Council of Medical Schemes 2016).

It has been widely acknowledged that the introduction of the Government Employees Medical Scheme (GEMS), a public service scheme, had a significant impact on the increase of paid membership since its launch in 2006, and its actions mobilised hundreds of thousands of civil servants throughout the years. An analysis of the figures in terms of contributions and expenditure per financial year provides interesting information for this study. Gross contributions until December 2016 amounted to R163.9b, an increase of 8.1% in comparison to the year before.

The gross healthcare expenditure on the part of medical schemes for the same period was R151.21b, an increase of 8.9% in comparison to the previous year. R56.61b or 37.44% of the amount was paid to hospitals (R56.32b to private ones, with an increase of 9.80% in comparison to the previous financial year). R10.15b was paid to 'allied' and 'supplementary' healthcare professsionals, showing an increase of 8.01%, while R 36.32b was paid to a wide range of specialists, with an increase e of 9.92% in comparison to the previous year. The amount was 24.02% of total medical aid payments made during the year. General practitioners received R8.96b or 5.93% of healthcare benefits paid, while consumables and medicines dispensed by pharmacists and providers (excluding hospitals), received R 23.95b (15.84% of benefits paid) (Council of Medical Schemes 2017).

R 73.1b was the total cost of prescribed minimum benefits (PMBs), while the total risk benefits reached R 136b or 54% of total risk benefits paid. R 11.9b was spent on administration and broker costs reached R2.0b, 10% more than the previous financial year.

A deficit of R 2.39b was reflected for all medical aid schemes, with R 955.7m for the 'open' ones and R 1 435.1b for the 'restricted' ones, the result of an increase in claims; net assets were R 54.1b. The sector's solvency ratio

decreased in 2016 to 31.6% in comparison to 32.6% in the previous year (Council for Medical Schemes 2017).

The public-service controlled medical schemes are classified as 'restricted medical schemes' and it has been estimated that more than 41% of medical schemes members in the country belong to such schemes. Despite the existing differences between the open and restricted schemes, both categories are legally bound by the dictates of the Medical Schemes Act of 1998.

While in the early years of the new Millennium there were at least 95 such schemes registered in South Africa, their number at present has shrunk to 60. One of the key reasons for such decline is that many of such entities have suffered from a number of weaknesses related to limited number of members, in-fighting amongst the leaders and lack of knowledge that could lead to sustainability **(Interview No. 1, Senior Public Servant, and Gauteng Province).**

In most cases, the restricted schemes have been small in terms of principal membership when compared to the open ones, and it is interesting to note that there are at least 25-30 such schemes that have been allowed to operate illegally, as they did not have 6000 principal members when they registered or at least until the end of 2015. The Government Employees Medical Scheme (GEMS) is the numerically and influence-wise largest restricted scheme, with more than 700 000 principal members and over 1.2 million dependents. It is the second biggest scheme in the country, controlling 17% of the market share, with DISCOVERY at 32% being the top-ranking company.

GEMS is followed by the South African Police (SAPS) scheme (POLMED), that has over 200 000 principal members and just under 400 000 dependents (Fin24 2017a). Transmed Medical Fund, that provides services to Transnet Group employees including those in the entity's present and past subsidiaries, accommodates the largest number of pensioners in comparison with other schemes (with average age of over 50 years), and its claims ratio in 2015 was 105.3%.

In terms of the proportion of contributions used to fund claims, in general, the risk claims ratio of restricted medical schemes (94.9%) has been higher than that of the open schemes (at 88.7%) in 2015. In 2015, restricted schemes spent 6% of their contribution income on non-healthcare expenditure, and open schemes spent just over 10%. Restricted schemes tend to be cheaper to administer, as the companies who employ the members often absorb some of the costs of running the scheme. They also do not pay any broker fees.

Of the restricted schemes, Sasolmed paid out just under R1600 in claims per member per month, Profmed just under R1400 and GEMS just over R1200. Profmed had the highest non-healthcare expenditure of the restricted schemes, coming in at over 16%.

The vast majority of the largest restricted schemes in the country (8 out of 10), did not have an operating surplus in 2015 (Transmed, Sasolmed. Nedgroup, Polmed, Platinum Health, Bankmed, GEMS and Profmed). With the exception of GEMS, all restricted medical schemes had a solvency level of over 60%, and two of them (Transmed and Platinum) had solvency levels below 25%, the recommended level (Fin24 2017b).

## Research Methodology

The utilization of the qualitative method and paradigm at the empirical level was the basis of the research project. This was rooted in a multiplicity of data collection patterns that involved the dissection of primary and secondary material including government and departmental documents, press and official reports, journal articles and books, as well as interviews with public and private sector officials. The anonymity and confidentiality of all participants were guaranteed.

The selection of the officials both in government and statutory professional bodies was based on the principles and implementation of the judgmental sampling technique. They were selected because of their expert knowledge and understanding of the research field.

The analysis of data took place through the use of descriptive and interpretative techniques based on content analysis that led to direct and/or indirect interpretation.

## Corruption in Medical Schemes: A Snapshot

The medical aid sector in South Africa has become a seriously 'concentrated'/ oligopolistic sector dominated largely by the 'BIG 3': MEDSCHEME, Metropolitan Health (MMI) and DISCOVERY that are in control of over 80% of all medical scheme membership (Fin24 2017b). Throughout the years, it has been replete with corruption and fraud. However, fraud and corruption affect all of the existing entities.

The most visible fraud and corruption reality in the medical aid scheme terrain is related to perpetual collusion between healthcare service providers and

medical aid members at all operational levels and throughout the sector. However, the corrupt relationships between medical practitioners, mediators, members and staff of both closed and targeted medical schemes, are also key in the fraud terrain **(Interview No. 2, Senior Public Servant, and Gauteng Province).**

Research by the Healthcare Forensic Management Unit (HFMU) of the Board of Healthcare Funders of Southern Africa (BHF) in 2015, has indicated that more than 7% of all medical aid claims in South Africa have, over the years, been fraudulent, with strong possibilities that such actions could reach the 15% of the claims received. This means that the principal members of any medical aid scheme are obligated to pay an additional amount of between R192 and R410 per month **(Interview No 5, Medical Scheme Board Member).**

It can be understood that such increases dent the financial security of lowly paid employees Department of Health 2017:39 - 40).

Such collusion is related to direct or indirect abuse of medical aid benefits and fraud wastage, and has been a challenge of major proportion in the sector for decades, with serious repercussions for the provision of quality-driven and affordable healthcare.

In quantitative terms, if an approximate amount of the R150b per year is spent in South Africa and 10% of claims are fraudulent; this results to fraudulent costs of R15b. Such realities affect every single stakeholder in the sector, and schemes and circumstances obligate them to work collectively in order to eliminate corrupt practices, especially the lower paid beneficiaries who are hard hit by these illegal acts. It is estimated that medical aids lose between R9 and R19b every year due to fraud, abuse and waste. A forensic analysis over a period of 5 years of the transactions of medical aid and consulted service providers through the use of the latest technology including forensic software algorithms able to identify corrupt acts and fraud, estimated that fraud has reached over R22b a year, meaning that members have lost more than R2500 due to fraud and corruption (Buthelezi 2017).

The industry has accepted that the culprits are members of an ever-increasing minority of uncaring, dishonest and corrupt personnel, operating in the form of informal syndicates involved in a number of practices that include acts such as fake invoices; charging excessively high levels of service than those delivered; submitting claims in false names; billing for services that have not been not provided; claims by pharmacies for genuine medication while dispensing generic medication; claiming from medical schemes for medicine while buying cosmetics, baby powders or other items; 'card sharing', as health pro-

fesssionals submit claims of non-members who use a member's card; fraud committed by healthcare professionals and service providers; provision of fake sick notes so the member can claim from the medical aid scheme, and fraudulent change of diagnosis so that a member can access specific expensive benefits. The so-called 'card farming' is a scheme whereby medical aid scheme members 'lend' their membership card for a fee or free of charge to non-members, who can then use them for a number of treatments or to purchase non-medical merchandise from pharmacies and submit the claims covering the costs to the scheme **(Interview No 6, Private Hospital Manager, Gauteng, October 2017).**

One of the more well-known and recent scams to hit one of the biggest private medical aids in South Africa, involves lump sums which are paid out by Hospital cash plans that are schemes operating by insurance companies. These companies provide members with lump sums of money when hospitalisation takes place, and are directly and indirectly abused through fraudulent schemes instead of helping to cover the shortfalls not fully covered by the medical schemes. The admission of people who are not sick to hospital, aided by private medical practitioners, helps the 'syndicate' members submit false claims to the schemes and the provider of the cash plan, who then split the lump sums involved with the medical practitioners. In all such cases, both the medical scheme and the insurer lose substantial amounts of money. It has become evident that fraud committed in the process of claiming for hospital cash plan benefits has been spread widely throughout the country. By 2014, the number of such plans fluctuated between 1-1.5 million, covering over 2.4 South Africans and with a monthly increase of 50 000 new policies monthly (Fin24 2013).

## Corruption in the Public Service Medical Schemes

It has been widely reported that while the open medical schemes, spear-headed by the 'Big 3' have attempted with what has been called 'notable successes' to curtail fraud and corruption in their operations (Greve 2017; Ensor 2018), this cannot be said of public service medical scheme providers. These are basically the ones that deal with the majority of beneficiaries who are state employees with fluctuating incomes and financial resources. These groups comprise mostly of lower to medium remunerated employees who when the cost of living increases together with their medical aid prices, they become financially vulnerable because their economic security and stability are threatened.

The reports of the widening spectrum of fraud in the sector were direc-

tly associated with the expansion and growth of the industry in a highly competitive environment and its expansion from KwaZulu-Natal to the Eastern Cape, provinces predominantly populated by public servants. Other provinces alerted a number of role players such as the relevant ombudspersons and the Association for Savings and Investment SA, which attempted to investigate the problem (Health24 2016).

The fraud that became evident especially since early 2011, and which has since expanded seriously, prompted Brian Galgut, the past Long-term Insurance Ombudsperson, to highlight the abuse of the schemes as the perpetrators' terrain had become more diversified and adventurous, boosted by a substantial new crop of medical service providers and practitioners involved in all schemes.

It can be understood that the expansion of such fraud and corruption will inevitably impact negatively on both the medical aids sector and especially their members, because both will, especially the latter group, incur additional costs in terms of increases in premiums for hospital cash plans for the members and higher expenses for excessive claims for the schemes. The firms will also face additional costs for investigations (*City Press* 2013).

Given these realities, it seems that a case study that received some publicity is merely a drop in the ocean of corruption. However, some lessons can be learnt after the fact.

The case of 200 members of the South African Broadcasting Corporation (SABC) was reported publicly without making news-paper headlines. Employees of the corporation colluded with a number of medical practitioners and service providers in order to commit fraud against the SABC medical aid scheme operated by Medscheme at the time.

Following the evidence, 134 staff members were charged and after the completion of the disciplinary processes, 123 of them were dismissed with immediate effect (Polity 2015). In many ways, such a fraudulent act, irrespective of its coordinated or uncoordinated nature, pales into insignificance when compared to the multi-million rand case of the Government Employees Medical Scheme (GEMS) recently. By 2017, GEMS had 1.833 million beneficiaries and is the scheme that provides medical cover to 57% of eligible public servants.

The corruption in the entity blossomed as substantial number of members and healthcare practitioners and companies were involved in fraudulent claims, including significant in-hospital claims. In the latter cases, the claims were fraudulent in respect of the length of admission and the complete lack of serious radiology or pathology or radiology tests while in

hospital. Most of the corrupt claims were directly related to benefits associated with hospital cash back plans.

Perpetual corruption at GEMS led the relevant regulatory authorities to believe that the scheme could be insolvent by the 2016 financial year and would be bailed out by the Treasury. Such a movement would be detrimental to the belief and ambition that it could be a model to be followed in the future realization of the National Health Insurance plan.

The fact that the Council of Medical Schemes did not put GEMS under curatorship after the failure to meet minimum statutory requirements of solvency ratio is significant. GEMS' ratio stood at 5% (the solvency ratio is 25%). Its 2016 deficit was R1.2b and its reserves 2%.

During 2016, GEMS raised the members' contributions from R1 389 to R1 764, a 21% increase (Norje 2016). By 2016, the GEMS website items, Fraud Zone, Blow the whistle on fraud! Fraud against GEMS, Fraud Forum, Types of fraud, Implications of fraud and Fraud Awareness, were ALL discontinued.

Perpetual fraud, corruption and mismanagement across the board in GEMS led hundreds of its members who felt the consequences of perpetual annual increases calling for the medical aid schemes' scrapping from the map, as they had been perpetually rejected by most medical practitioners. There was evidence presented that fraud and corruption within the organization had led to the medical aids of members becoming exhausted as early as February and many of them turned to bank loans or 'mashonishas' (money lenders). This meant that members could not use their benefits and were subsequently rejected without any medical service and facilities.

The newly established Educators Union of South Africa (EUSA) stated on the day of their recognition from the Labour Department, that one of the key objectives of the union was the complete scrapping of the corrupt GEMS and that they had planned country-wide picketing demonstrations demanding its immediate closure by the state (EUSA 2018).

There have been cases where large numbers of GEMS members witnessed their funds being 'exhausted' after two months and large numbers of medical practitioners and pharmacies refusing to accept the medical scheme's cards. A few days after its official registration, hundreds of the union's members held picketing demonstrations outside GEMS offices together with ambulances representing SARAESA (the South African Private Ambulance and Emergency Services Association), medical practitioners representing NHCPA (the National Healthcare Professionals Association). All constituencies called for the immediate scrapping of the medical scheme (Masuku 2018).

Perhaps the most 'daring' corruption act committed by GEMS was exposed through its 'collaboration' with a private public relations company, which provided 'free medical advice' online to the medical scheme's members. The service was called 'House Call with Dr. Joe' and operated since 2014. It was advertised as a personalised health care advice column and was 'managed' by Martina Nicholson Associates, who handles public relations for GEMS and a number of other medical schemes. While the firm insisted initially that medical practitioners were employed, it surfaced that it was company employees who answered questions on depression, fertility, cancer, pharmaceutical needs, and infections, through the use of GOOGLE. Although GEMS and the public relations company insisted that all responses were written and signed by two medical doctors and provided 'proof' of such transactions, three independent medical practitioners showed that many answers were incorrect, a fact verified in the process by employees of the public relations company. In the process of investigating the case, a number of medical practitioners pinpointed many unscientific and incorrect responses provided that dealt with serious health conditions and diseases such as breast cancer risk, children's Attention Deficient Disorder, HIV/AIDS, diabetes and birth control, children's recurrent pneumonia, as well as 'cut and paste'-based wrong answers provided by 'Google services'. In fact, as the story unfolded, without really hitting the headlines, both GEMS and the public relations company insisted that this was just an 'educational guide' for members and not 'medical advice to patients'.

Such a 'defensive' position hid the fact that the pretention of those operating the system was not only unethical and illegal in their totality, but according to the Health Professions Council of South Africa, committing a 'criminal offence'. According to the Health Professionals Ethics Conduct of 2010, only registered and competent are authorized to take part in any form of tele-medicine practice in the country (Child 2017).

Despite the fact that there have been efforts to fight fraud and collusion through cooperation and open communication in the 'restricted' schemes, and there were existing arrangements in place for sharing information and reporting fraud and collusion, in 2016 less than half of the schemes utilised estimates of losses to increase their anti-corruption capabilities. This could have been achieved through a careful dissection of the existing detected realities and the training of specialist staff to deal decisively with fraud and corruption. At the time, less than 30% of them provided such training to the staff dealing with and fighting corruption and fraud, despite all of them having introduced anti-fraud and corruption policies **(Interview 5, Medical Scheme Board member).**

Things have improved somehow through the schemes' collaboration with the Healthcare Forensic Management Unit (HFMU), which has been helpful in decreasing the existing collusion, corruption and fraud risks to a certain extent, hoping to achieve in the future the total eradication of the scourge. They have been instrumental in increasing the communication channels and information sharing in the sector to a large degree (Fin24 2015).

While collusion has been there almost from the first day of the sector's existence, there are corrupt practices associated with the very governance and operational realities of medical aid schemes that have existed for many years. One of those well-known is the exorbitant 'stipends' that the scheme trustees pay themselves, obviously through the 'utilisation' of member contributions. Trustees are people who under 'normal circumstances' would be supposedly volunteering their occasionally valuable services. One of the reasons for such deeds is the fact that existing legislation does not provide rules, regulations or guidelines that monitor, evaluate or determine trustees' 'stipends' or other forms of payment. Given this situation, it is understandable that such money is paid for remuneration associated with attendance at meetings, travel, meals, accommodation and similar expenses. A comparative view of such processes paints the picture clearly.

According to the 2013 CMS annual report, the trustees of the then top six medical schemes received R25 021 000 each. The interesting detail of the comparison pointed to the fact that GEMS notably, the Government Employees Medical Scheme, or the *public sector* medical scheme) had the highest cost of R795 100 (Council for Medical Schemes' Annual Report 2013). The average remuneration per trustee was R568 000. Fedhealth, Hosmed, Bonitas, and Discovery paid an average of R 3 600 000 per year to trustees.

In 2016, DISCOVERY overtook GEMS in comparison and paid an average of R673 000 to all six trustees. The corruption- and scandal-ridden GEMS was relegated to second, paying R597 000 to its 12 trustees (double the number in comparison to the private sector operators).

The leadership of the financial supervision of CMS has been on record as indicating that such extravagance in 'stipends' was a serious concern for the entity, which was reinforced through comparative research undertaken by the council in collaboration with a reputable tax and advisory firm EY. The research, broadly based on the unpacking of remuneration of trustees, considered the 'stipends' exorbitant and dealt seriously with the weaknesses of the Medical Schemes Act and especially its Regulation No. 6, that needed urgent review. The role of the Registrar of the Medical Aid Schemes should

also become more instrumental in the determination of trustee remuneration (Council for Medical Schemes' Annual Report for 2016). This is one of the key issues facing medical aid schemes in terms of governance, and the reality is that despite continuous efforts on the part of the Council for Medical Schemes and its Compliance and Investigations Unit to rectify such situations, it is almost chronic (Council for Medical Schemes' Annual Report 2014). By its own admission, the sector's statutory body, which has the duty and responsibility to regulate it, lacks the authority charged with regulating the industry and has not been able to make a significant positive change in respect of the present poor governance.

Over the years, there have been a number of medical aid schemes that have been placed under curatorship most in the restricted category indicating the poor management and leadership that is the ultimate foundation of bad or weak governance.

The question that arises, then, is what the exact role of the very well-paid trustees in tightening governance is, given the fact that the stipend of a number of trustees of schemes under curatorship has been almost doubled in a short period of time. There have been members' complaints of serious manipulation in trustees' appointments and their continuous abuse of overseas trips, inordinate fees, and other excesses (Fin24 2015a).

Despite the fact that the CMS leadership and relevant organs have been working for seven years towards a plan determining guidelines of remuneration for trustees, as well as training in respect of their obligations, duties and responsibilities, no outcomes have been achieved at present.

The record shows that there have been a number of issues directly connected to the current status of poor governance especially in terms of the restricted medical schemes, such as lack of active membership participation at Annual General Meetings, which are in most occasions inaccessible or badly timed; poor attendance and lack of interest on the part of members; lack of appropriately structured agenda items; lack of transparency on the part of trustees and the schemes in general; lack of continuous communication with scheme members, and the absence of direct information to members on their own duties, responsibilities and obligations (Council for Medical Schemes' Annual Report 2014).

It has become evident that lack of member interest and public participation is a significant reason for the perpetration of bad governance that, according to the CMS, is also affected by a number of gaps in the existing key legislation. The entity in 2004 put forward a number of amendments to the

Medical Schemes Act of 1998, aiming at strengthening the foundations of governance of the medical aid schemes. The amendments were withdrawn as the leadership of the Council supported the government's focus on the NHI (the National Health Insurance), but new hopes were raised when the act was back for consideration **(Interview 5, Medical Scheme Board Member).**

For a number of years and on a number of occasions, the CMS included a section called '*Undesirable business practices',* where specific incidents of poor and bad governance practices and corruption were identified, including this item in Section 61(3) of the Medical Schemes Act. These were the results of inspections identified in Section 44(4) (a) of the same Act. Over the years, the inspection discovered, amongst other things mainly in the restricted medical schemes, 'irregular payments to consultants'; removed trustees spending R27m of the scheme to 'fight their removal'; 'remuneration for three members to the extent of R1.8m while fighting against their removal; fraud, misconduct and other irregularities; interference by the employer in scheme affairs; schemes' refusals to allow governance issues to be investigated; illegal dissolution of audit and risk committees, and illegal payments for the principal officer and the trustees for entertainment (the Cape Town Jazz Festival). During one financial year, there were 10 investigations and one High Court case Council for Medical Schemes' Annual Report 2012; 2013; 2014; 2015).

While fraud, corruption and collusion in the sector has escalated, according to leaders and functionaries in the industry, reaching on many occasions highly sophisticated levels, the lack of utilisation of appropriate technological innovations exacerbates the problems despite the existence of international analytics devices that are able to fight waste, abuse and fraud. Such devices are able to provide identification of potential and/or existing abuse and fraud through a dissection, analysis, monitoring and evaluation of irregular claiming patterns leading to detection, planning and subsequent action. Detection leads to further investigation by specialists in forensics, followed by the company's calculated action **(Interview 3, Senior Public Servant, Gauteng Province).**

Given the fact that in all these cases it is not only medical service providers in conjunction with medical scheme members that commit corrupt acts, but on many occasions medical scheme employees who are involved directly or indirectly, there are operational and organisational realities that create the foundations of corrupt activities. This is especially the case of the restricted ones.

There has been evidence that the complexity and vast volumes of medi-

cal aid claims data every day are becoming a burden to the complex operational systems and are used or abused for corrupt and fraudulent acts **(Interview 4, Senior Public Servant, Gauteng Province).** This means that such volumes of electronic data daily make it extremely difficult, especially for inadequately skilled or corrupt employees to understand, detect and stop fraud. Such realities are exacerbated by the lack of fraud and risk management.

Terabytes of claims data reach medical schemes and are in need of processing and these need to be supplemented by pressures of continuous reporting, thus creating serious problems for risk management departments, especially in restricted schemes, which lack urgency and prioritisation of information technology, as well as personnel or skills in forensic data analysis (News24 2015).

It is accepted within the industry, that although the 'open' schemes have significantly updated their efforts to ratify the weaknesses of their organisational and administrative systems to mitigate fraud and corruption, the same cannot be said about the 'restricted' ones. The complaint lodging avenues of the latter, when their organisational mechanisms establish solid reasons for reporting fraud, are with the professional councils and the South African Police Services. Such actions mean that in most cases, investigation proceedings last very long, as most anti-corruption agencies, including SAPS, have over the years faced serious challenges in terms of prosecuting perpetrators of fraud and corruption. Thus medical schemes generally struggle to get fraudsters convicted for a number of serious reasons. Such realities allow fraudsters and corrupt staff, medical practitioners and service providers and members, to continue unabated **(Interview 5, Medical Scheme Board Member, Gauteng Province).**

Detection, monitoring and prevention of corruption in medical aid schemes is complex and fragmented, as different schemes, especially the public service ones, are operating in isolation and have not consolidated their efforts to fight fraud and corruption. Such a reality is the result of intense competition amongst different schemes, as those who succeed in fighting corruption create an aura of success and competitive advantage (Mothudi 2018:13).

## Conclusion: What is to be Done?

Corruption at all levels of society has a wide number of negative effects such as the depreciation of the rand, leads to the depreciation of the national currency, become a serious barrier to local and foreign investment reduces funding for health, education, infrastructure and depreciates national currency, and cuts

down on public servants' wide variety of benefits such as medical aid. All these have a direct and indirect negative effect on the financial security and lives of the vast majority of the working and middle classes, including the public servants.

The almost perpetual depreciation of the rand because of corruption and political instability has direct and indirect effects on a number of health related products and services such as pharmaceutical, hospital expenses and medical aid scheme, especially the public sector ones (Woods & Mantzaris 2012).

So much is the South African stated concerned about corruption, abuse, waste and fraud, at all levels, services and products in both the private and public health care systems that the Head of SIU (the Special Investigating Unit) announced publicly that the Unit after a meeting in Pretoria announced the establishment of whose forum would be the fight against fraud, waste and all forms of corruption in all sectors of the healthcare terrain.

The new forum would be an integral part of the expanded ACTT (the Anti-Corruption Task Team, a multi-department team established as a new entity in 2009 aiming at meticulous detection, investigation and prosecution of all alleged cases of corruption in the sector.

The Task Team's original mandate was expanded in 2014 in order to include a number of other programmes, that included intelligence, policy support and crime operations (Mabuza 2018)**.**

The realities identified in the article point to the truth that despite a number of successes in the relentless fight against fraud and corruption in the medical aid scheme terrain on the part of the operating in the free market sector, the same cannot be said of the 'restricted' ones. This fact continues to dent the financial security of all beneficiaries belonging to the working class and lower and middle-class categories of public servants.

A key solution that is urgently needed is a final and well-articulated decision of the leadership of all medical aid schemes, especially the public service ones, to unite as an industry and decide to join operations in the fight against fraud and corruption in their midst.

Such a decision will go a long way in showing the ever-growing membership that the schemes have realised that fraud and corruption are a major threat to the entities' existence, as well as the well-being of over 9 million members.

It is essential that the individual efforts of schemes and administrators are consolidated in an industry-wide central database to facilitate collective use and analysis of data, as it is done, for example, in the banking sector. The

Council for Medical Schemes can be instrumental in such a move as it is evident that fraud and corruption seem to be posing a serious threat to the medical schemes and their potential to save over R10b that is currently lost through fraud and corruption.

The success of medical aid scheme risk management, investigation detection and prevention at present is directly connected to the existence of solid technological assistance, what is known as 'back-end technology' and the 'big data innovations' that are instrumental in stream-lining and improving the anti-corruption environment that leads to easy and quick detection.

The new technological innovations characterized by up-to date analytical tools have been instrumental in dissecting data in effective ways. Advanced technology is an enabler of real-time mining of data, allowing the schemes to track and monitor member and provider profiles and actions, thus detecting fraud. Fraudulent behavior leading to fraud is tracked as identification of perpetrators becomes a reality, immediately enabling schemes to act decisively.

The latest preposition of the Council for Medical Schemes for the future consolidation of all public service employees into GEMS, has led to an occasionally healthy debate on the issue. This is not enough. A concerted effort to determine the best way forward is essential so that the long term financial security of all members is guaranteed. It is evident that a future consolidation of such a nature is in line with the governmental policy guidelines of the National Health Insurance. Given the existing realities in this terrain, it is most likely that strong opposition will be faced by both open and closed entities as well as the members themselves, given the dynamics, actions and inactions, as well as the behavior of the GEM's leadership.

However, such a decision will call upon each and everyone in the medical aim scheme terrain to answer the question: 'If the answer is 'no' how much do you really care about the wellbeing and financial security of all your members?'

The state contributes significantly to public servants' medical scheme contributions. Inevitably, workers belonging to active and strong trade unions will ultimately resist such steps that are seriously considered to be against their existing benefits. This is an issue of contention as the representation of over 30% of the industry members will operate under one 'roof' that will 'absorb' 10 schemes, including fraud-prone entities such as Rand Water and SABC. There is no doubt that a consolidated medical scheme would be ultimately beneficial as it could offer better savings and have stronger negotiating powers. Given its numerical strength, GEMS is possibly the best option. However, its

history and present disrepute are negative factors, raising suspicion especially if compared with Polmed, which is also numerically strong.

The possibilities of 'fast-tracking engagement strategies', where one or two schemes are used as 'experiments in the amalgamation' have no chance of success, because of history and existing particularities and differences. Only an open, frank and transparent debate amongst all stakeholders and role-players can lead to a consolidated public service medical scheme.

While the accusations and realities regarding the role of medical schemes and administrators in bullying the medical providers and patients are still prominent and confirmed in the past the state entities and administrators are legally obligated to look after and safeguard the funds of their beneficiary members and be in the forefront of the fight against abuse. They must come and act clean through their committed action to recover funds and thus help their members' financial by keep annual increases of medical aid under control.

## References

Auditor General 2017. PFMA Report. Pretoria.

Buthelezi, L. 2017. Deloitte Study Reveals Extent of Medical Claim Fraud. Available at: https://www.iol.co.za/businessreport/economy/deloitte-study-reveals-extent-of-medical-

Claimfraud-1499168. (Accessed on 18 March 2018.)

Child, K. 2017. Gems Accused of Using 'fake' Doctors to Give Medical Advice. 26 September. https://www.dispatchlive.co.za/news/2017-09-26-gems-accused-of-using-fake-doctors-to-give-medical-advice/ (Accessed on 29 March 2018.)

Council for Medical Schemes 2013. Annual Report 2012 – 2013. Pretoria.

Council for Medical Schemes 2014. Annual Report 2013 – 2014. Pretoria.

Council for Medical Schemes 2015. Annual Report 2014 – 2015. Pretoria.

Council for Medical Schemes 2016. Annual Report 2015 – 2016. Pretoria.

Department of Health 2017. National Health Act, National Health Insurance Policy: Towards Universal Health Coverage. (White Paper.) 28 June 2017, June 20. Pretoria: Government Printers.

Ensor, L. 2018. Efficiency behind Discovery's Health, says CEO. *Business Day* July 6.

EUSA 2018. Advancing our Members' Rights. Available at:

http://eusaunion.co.za/news/union-to-advance-teachers-rights/ (Accessed: on 29 March 2018.)

Fin24 2017a. Revealed: South Africa's Biggest Medical Schemes. Available at: https://www.fin24.com/Companies/Health/revealed-sas-biggest-medical-schemes-20171013 (Accessed on 24 April 2018.)

Fin24 2017b. Sources: Alexander Forbes Diagnosis 2016/ 2017. Restricted Medical Schemes in South Africa: 15 Facts that You Need to Know. Available at: https://www.fin24.com/Money/Health/restricted-medical-schemes-in-sa-15-facts-you-need-to-know (Accessed on 11 July 2018.)

Greve, N. 2017. Don't do Business with Corrupt Companies. Available at: https://www.fin24.com/Finweek/Business-economy/dont-do-business-with-corrupt-companies-discovery-ceo-20170929 (Accessed 07 July 2018.)

Mabuza, E., 06 June 2018. Elite Investigators to Target Healthcare Fraud and Corruption. Available at: https://www.timeslive.co.za/news/south-africa/2018-06-06-elite-investigators-to-target-healthcare-fraud-and-corruption/ (Accessed on 14 July 2018.)

Masuku, S. 2018. Calls to Scrap Government Employees Medical Scheme Growing. *Daily News* 15 May.

Mothudi, K. 2018. Collaboration and Analytics Vital in Combatting Medical Scheme Fraud. *CMS News* 1,1: 11 - 17.

News24, 23 November 2015. The Shocking Truth about Medical Aid Fraud in South Africa. Available at: https://businesstech.co.za/news/business/104953/the-shocking-truth-about-medical-aid-fraud-in-south-africa/ (Accessed on 11 July 2018.)

Norje, B., 22 August 2016. State Medical Aid May Go Bust. Available at: https://www.businesslive.co.za/bd/companies/2016-08-22-state-medical-aid-may-go-bust/ (Accessed on 24 January 2017). https://doi.org/10.1044/leader.PPL.22012017.24

Russell, J. 2015. Health Care Tops Lists of False Claims Act Violations. *Chicago Tribune* 2015. Available at: http://www.chicagotribune.com/business/ct-health-fraud-tops-list-1208-biz-20151207-story,amp.html (Accessed on 21 February 2018.)

Salter, M. 2010. Lawful but Corrupt: Gaming and the Problem of Institutional Corruption in the Private Sector. Available at: http://www.hbs.edu/research/pdf/11-060.pdf (Accessed on 28 January 2018.) https://doi.org/10.2139/ssrn.1726004

United Nations 2017. Right of everyone to the Enjoyment of the Highest Attainable Standard of Physical and Mental Health. Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/72/137 (Accessed on 22 April 2018).

Whistleblowers International 2016. Upcoding: Health Care and Medicare Fraud. Available at: https://www.whistleblowersinternational.com/ (Accessed on 30 March 2018.)

Woods, G. & E. Mantzaris 2012. The Anti-Corruption Reader. Stellenbosch: Anti-Corruption Center for Education and Research. ACCERUS, School of Public Leadership, Stellenbosch University.

## Interviews

Interview No 1. Senior Public Servant, Gauteng Province, Johannesburg. (18 October 2017.)

Interview No 2. Senior Public Servant, Western Cape (26 October 2017.)

Interview No 3. Senior Public Servant, Gauteng Province, Johannesburg. (19 October 2017.)

Interview No 4. Senior Public Servant, Gauteng Province Johannesburg. (17 October 2017.)

Interview No 5. Medical Scheme Board Member, Gauteng Province, Pretoria. (19 October 2017.)

Interview No 6. Private Hospital Manager, Gauteng. (21 October 2017.)

Professor E.A. Mantzaris
Retired Professor
Mangosuthu University of Technology
Durban
South Africa
evangelos.mantzaris@gmail.com

# Chapter 4: Can BRICS Contribute to Global Peace and Security?

**H.H.S. Viswanathan**

## Abstract

Peace and Security is the sine qua non for progress and prosperity. History has shown repeatedly that countries and regions have prospered only during periods of peace and stability. The grouping of BRICS (Brazil, Russia India, China and South Africa), which, to begin with, was a geo-economic entity has, over the last decade, expanded its agenda and grown into an influential force. It discusses geo-political issues and has not shied away from expressing its views on several ongoing conflicts. Over the last ten Summit Declarations, the number of paragraphs dealing with Peace and Security has steadily gone up. The question that arises is whether BRICS can take a larger role in the maintenance of Global Peace and Security?

As a group claiming to bring in a new narrative of the Global South for Sustainable Development, it cannot stay away from issues that affect such development. In many areas of the world, economic growth, livelihoods and prosperity are hampered by insecurity and violence. Can BRICS address these issues effectively? There are, of course, many challenges. Firstly, BRICS is not even a formal alliance; how could the five formulate and implement policies?

Secondly, there are geo-political considerations of the five, particularly of India, China and Russia, which may not be similar. Nonetheless, the five could find common ground on some low-hanging fruits, which are of interest to all. These could be Peacekeeping, Peace Building, anti-piracy, action against drug and human trafficking and anti-terror activities. BRICS could also address factors that lead to conflicts namely the non-traditional security threats like poverty, youth unemployment, non-inclusive growth, increasing disparity between the haves and the have-nots, food and energy security. A new narrative shifting the focus from conflict resolution to conflict prevention is the need of the hour. Peace should be seen not only as absence of conflicts but also as absence of all factors that could lead to conflicts.

If BRICS has to play a greater role in Peace and Security, it should also

gain greater voice in the global mechanisms and platforms dealing with these issues.

On balance, it is clear that the time is ripe for BRICS to have a long-term perspective and venture into Peace and Security Initiatives in an incremental and calibrated manner.

**Keywords:** BRICS, Global Peace and Security, new narrative of sustainable development, Peacekeeping, Peace Building, anti-piracy, action against drug and human trafficking, anti-terror activities

## Introduction

Peace, Stability and Security are the sine qua non for economic development and prosperity. A clear lesson that one draws from history is that periods of economic well-being of societies have coincided with those with peace and stability. This is obvious because any short- or long-term planning for progress in the economic or cultural fields is impossible in an atmosphere of violence and conflicts.

The importance of Peace and Security has been reflected in the formulation of United Nations' Sustainable Development Goals (SDGs) in 2015. SDG 16 is devoted to this aspect of development[1].

There is another reason why Peace and Security is critical for development. In an inter-connected world, conflicts and instability have a tendency to spread across regions. The most recent examples of this can be seen in West Asia and North and West Africa. The instability in Syria had its origin in the Iraq crisis. The instability in Libya following the overthrow of Gaddafi had its repercussions in Mali.

This paper seeks to explore the possibilities of a grouping like BRICS (Brazil, Russia, India, China and South Africa) contributing to Global Peace and Security. The group started as a geo-economic group; however, over the last decade, it has gained enough global influence to expand its agenda to include geo-political issues. Is the group now in a position to address Peace and Security problems? What kinds of security issues are they capable of handling?

[1] United Nations. 'Transforming our World: The 2030 Agenda for Sustainable Development' (2015). https://sustainabledevelopment.un.org/post2015/transformingourworld

What are the major challenges the group is likely to face? Will the geo-political considerations of the five affect a common strategy? Do they have to take a new and novel approach to the question of Peace and avoid age-old concepts like balance of power et al? These are some of the critical questions requiring clear answers.

## Evolution of BRICS

When Jim O'Neil of Goldman Sachs coined the term BRIC in 2001 to include Brazil, Russia, India and China, he was identifying the most promising investment destinations for the benefit of the investment banks (O'Neill 2015). Over the last seventeen years, the group has grown in strength and is no longer just good investment destinations. In the first few years, there were only informal consultations. In 2009, the first Summit level meeting was held in Ekaterinburg in Russia. South Africa was added to the group in 2011. The agenda of BRICS kept expanding with each Summit. Broadly, three sets of issues were the focus of the group, viz.,

(1) intra-BRICS Cooperation in a whole range of sectors critical to the five countries like health, education, sustainable development, inclusive growth, gender parity, food and energy security and climate change;

(2) reforming Global Financial Institutions particularly the International Monetary Fund (IMF) and the World Bank (WB) to improve its functioning and make them more representative to reflect the current economic reality of the world; and

(3) BRICS's keen interest in addressing the larger Global Peace and Security and Opportunities.

## Governance Issues Including Redefining Values and Norms

Intra-BRICS trade has grown in the last fifteen years even though it is nowhere near the true potential. Social sectors like health, education, urbanization, inclusive growth and gender parity have also seen meaningful cooperation by way of learning from each other's experiences and following best practices.

On the question of reforming Global Financial Institutions, some progress was achieved at the G-20 meeting in Seoul. There was some increase

in the voting powers of BRICS; however, further movement on the issue has been blocked by the US Congress. There is a lot of ground still to be covered. BRICS, in the meantime, have taken the initiative to create alternative institutions. The establishment of the New Development Bank (NDB) and the Contingency Reserve Arrangement (CRA) in a short period of three years is indeed a remarkable achievement for the group. Even though these are not envisaged as rivals to IMF and WB, but as additional mechanisms, the political message is very clear. It is for the first time in the last two hundred years a global institution has been established without the participation of 'the West'. The other message was that outdated Global Institutions which refuse to change and adapt could soon become irrelevant.

Today BRICS is talking of further initiatives like its own Credit Rating Agency, standards and bench marks.

The above shows clearly that on the economic front, BRICS has made a mark and accumulated sufficient heft. What about the political front? Has there been a commensurate increase there? Initially, there was none since BRICS started as a geo-economic group. Nonetheless, the situation changed very quickly. Starting with the Summit in Sanya (China), the final Summit Declarations have increasingly addressed geo-political issues. It was clear to everyone that BRICS would not hesitate to give its views on the burning international political and strategic problems of the day. What started as references to the Libya and Iraq situations in Sanya grew in content over the subsequent Summits to cover diverse issues like Syria, Terrorism, Extremism, Cyber Security, Peacekeeping and Peace Building.

With this background and evolution, today BRICS cannot shy away from Peace and Security issues. Of course, there are different kinds of security related issues. Which are the areas where BRICS can effectively intervene? What are the challenges?

There are certain aspects of BRICS, which make the group an ideal candidate for taking a leadership role in Global Peace and Security. These flow from some of the fundamental principles to which BRICS attaches great significance. *One* is the strong opposition to the use or threat of force from these countries.

The *second* is their firm belief that Peace and Stability are closely associated with development and economic prosperity. The *third* aspect is the centrality that they attach to the United Nations in dealing with global issues. The *fourth* is their strong belief in multilateralism as a tool for solving inter-

national problems[2].

While talking of the importance that BRICS attaches to the United Nations (UN) and Multilateralism, we should remember that BRICS cannot agree to a status quo of these principles. It is a fact that in the last seven decades, both the UN and Multilateral Diplomacy have been dominated by the West. While BRICS sees the necessity of the two aspects as fundamental to international relations, the group also strongly feels that both need modifications and reforms. Ideally, BRICS would work for the centrality of a reformed UN and an updated version of multilateralism. There should be no objection from most of the international community in accepting these principles. Consequently, a major role of BRICS in Global Security could be seen as a positive move.

## Kinds of Cooperation Possible in Security Related Issues

It is clear that BRICS are in the beginning stages of dealing with Peace and Security. It is therefore important to understand the different kinds of possible cooperation. The first and the simplest is coordination of positions. The group can articulate a common position on some of the burning security issues of the day. Even this would involve some dialogue and negotiation between the five because of each one's perception of the problem and its own geo-political considerations. The next level is coordination of policies. This would require a higher degree of common commitment to the issue and a clear consensus on the course of action. Then comes the Joint Implementation of the decided policy. Here, there is the requirement of a clear division of duties agreed to by all. The last level is the building of new Institutions to formalize the cooperation (Abdenur 2017).

BRICS, as of now, is a long way from joint implementation of policies or building institutions in the security area for reasons that we shall discuss under the challenges to BRICS playing a more significant role in Global Peace and Security. However, BRICS have made a small beginning in the area of coordination of positions. As we shall see later when we analyse the various Summit Declarations, over the last decade, there has been considerable coordination of positions on issues like Iraq, Syria, Terrorism, Cyber Threats, Drug and Human Trafficking and Piracy. Yes, it is true that this coordination of positions has not resulted in concrete action yet.

[2] In all BRICS Summits' declarations, the centrality of multilateralism is implied.

## Evolution of the Subject of Peace and Security in the BRICS Summits

As has been mentioned earlier, BRICS was conceived initially as a geo-economic group. Therefore, security issues were peripheral to the main discussions in BRICS. This was also necessitated by the timing of the first two Summits. The first one in Yekaterinburg in Russia was held in 2009 soon after the Global Financial Crisis of 2008. Naturally, the main preoccupation of the four (South Africa had not become a member yet) was to find ways of minimizing the fall-out of the crisis on their economies which had been growing at impressive rates for over a decade. The same trend continued in the Summit in Brasilia in 2010. There was hardly any mention of security related issues; however, there was a fleeting reference to Terrorism. It was from the Sanya (China) Summit in 2011 that the BRICS Declarations began discussing geo-political, strategic and hard-core security problems. The Sanya Declaration referred to crisis affected regions such as the Middle East, North Africa and West Africa. There was a coordination of position on the Libyan crisis[3].

By the time of the New Delhi Summit in 2012, many of the crisis affected areas had reached critical levels. For the first time for BRICS, the term 'Security' finds a place in the New Delhi Summit's main theme which was 'BRICS Partnership for Global Stability, Security and Prosperity'. In the Declaration, issues pertaining to international security made up nearly half the total number of paragraphs[4].

The eThekewini (South Africa in 2013) Declaration had very few security related references. This was understandable since as a new member South Africa wanted to make a mark and they chose to give priority to the regional development of the Africa. Their wish was to be a spokesman of the Continent in the BRICS Forum and explore the group's contribution towards economic development of Africa[5].

---

[3] Sanya Declaration on BRICS (2011). https://www.brics2017.org/English/AboutBRICS/DOPS/201701/t20170114_1116.html

[4] BRICS Delhi Declaration (2012). https://mea.gov.in/bilateral-documents.htm?dtl/19158/Fourth+BRICS+Summit++Delhi+Declaration

[5] BRICS eThekwini Declaration (2013). http://www.brics2018.org.za/sites/default/files/documents/eThekwini%20Declaration.pdf

At the Fortaleza (Brazil) Summit in 2014, many security related issues came into the forefront. There was prominent mention of Boko Haram's abduction of school girls and other atrocities as well as the deteriorating situation in the Middle East. There was also a concern about arms in Outer Space. The crisis in Crimea was at its height at that time and the Declaration had a significant para on that[6].

In Ufa (Russia) in 2015, under the Russian Presidency, there were many critical references to larger security issues. The Declaration categorically condemned Unilateral Interventions (obviously with the USA in mind) and argued for security for all. It went on to say that 'No state should strengthen its security at the expense of the security of others'[7].

India's desire in Goa in 2016 was to have a stronger language on Terrorism with mention of specific terrorist organizations in various regions including those in Pakistan responsible for terrorist activities against India. China was totally opposed to such a move since it would amount to letting down its staunch ally. As all decisions in BRICS are by consensus, India could not push it beyond a point. There was considerable criticism in some of the Indian media for India's failure to have the Pakistani terrorist organizations like the Lashkar-e-Taiba (LET) and Jaish-e-Mohammad (JEM) mentioned in the final Declaration[8].

The above issue got resolved in the next Summit in Xiamen (China) in 2017. To the surprise of many, China as the Host agreed to mention various specific terrorist organizations including those based in Pakistan. There have been many speculations on why China did what it did including one suggesting that it was China's way of sending a signal to Pakistan that it cannot be taken for granted. It is significant that the subject of International Peace and Security featured prominently in the final Declaration with 25 paragraphs devoted to the topic. Apart from Terrorism, other issues that got a mention are reform of UN

[6] BRICS Fortaleza Declaration (2014). http://www.brics2018.org.za/sites/default/files/documents/Fortaleza%20Declaration.pdf

[7] BRICS Ufa Declaration (2015). http://www.brics.utoronto.ca/docs/150709-ufa-declaration_en.html

[8] BRICS Goa Declaration (2016). http://www.brics2018.org.za/sites/default/files/documents/Goa%20Declaration.pdf

Security Council, Syria, Palestine, Iraq, DPRK, Iran Nuclear deal, instability in parts of Africa and drug trafficking[9].

The 10th BRICS Summit in Johannesburg in July 2018 came out with a Declaration which had 15 paragraphs under the Chapter 'Strengthening and Consolidating BRICS Cooperation in International Peace and Security'. The stress on Terrorism in the earlier Declaration of Xiamen was muted. No specific terrorist groups were mentioned. There were references to troubled areas like Afghanistan, Syria, Iraq, Palestine and Yemen without any new approach. A new and interesting reference was to the cooperation between the United Nations Security Council and the African Union Peace and Security Council. BRICS commended the African Union's commitment to the 'Silencing of the Guns by 2020' and supported efforts to strengthen the African Peace and Security Architecture. This must have been due to South African Initiative and is a good beginning for working towards concrete cooperation[10].

## Peacekeeping and Peace Building

All five countries have been active in this field. The commitments have steadily increased over the last decade. This area of activity needs two kinds of resources: financial and human (de Souza 2015). While the West has been stepping back in its involvement in Peacekeeping, the niche is being increasingly filled by emerging countries. As of April 2018, India ranks highest with 6,693 peacekeepers followed by China with 2,500, South Africa with 1,231, Brazil with 271 and Russia with 82[11]. India has traditionally been an enthusiastic participant in UN Peacekeeping operations. So far, it has

[9] BRICS Xiamen Declaration (2017). http://www.brics2018.org.za/sites/default/files/Documents/Xiamen%20Declaration.pdf

[10] BRICS Johannesburg Declaration (2017). http://www.brics2018.org.za/sites/default/files/Documents/JOHANNESBURG%20DECLARATION%20-%2026%20JULY%202018%20as%20at%2007h11.pdf

[11] Contributors to UN Peacekeeping Operations by Country and Post, as of 30 April, 2018. https://peacekeeping.un.org/sites/default/files/1_summary_of_contributions_2.pdf

participated in 39 operations with more than 100,000 soldiers in total[12]. India's three all-female police units in Liberia after the civil war was universally appreciated. Russia leads in number of UN Military Observers. Additionally, Russia has been contributing equipment such as heavy-lift cargo planes and helicopters. Other initiatives have been in the field of training of peacekeeping personnel. There is an important Training Centre in New Delhi (India) and a similar one in Brazil[13].

In terms of financial contributions, China and Russia lead the way with China making up 10.25% and Russia 3.99% of the 2017-2018 peacekeeping budget[14].

One fundamental principle that all the five countries follow is the necessity of a UN mandate for intervention or Peacekeeping. They are all opposed to unilateral actions, which bypass the UN.

The 10th BRICS Summit Johannesburg Declaration also says (para 52) that the leaders 'recognize the need for the South African initiative for a BRICS Working Group on Peacekeeping'[15].

Closely connected with Peacekeeping is the concept of Peace Building. This becomes critically important after a temporary peace is established through Peacekeeping. It involves bringing the warring sides together through negotiations and incentives. One primary requisite for this role is the credibility of the Peace Builder as an honest broker. BRICS can have this credibility except in a few specific areas of conflicts where the geo-political interests of some of them come into play. Take Africa, for example. The five can take peace building initiatives in conflict ridden countries with, of course, the approval of the concerned governments.

---

[12] India and United Nations Peacekeeping and Building (2018). https://www.pminewyork.org/pdf/menu/49151pkeeping.pdf

[13] Center for United Nations Peacekeeping (CUNPK) New Delhi, India (2018). http://www.claws.in/cunpk.php

[14] United Nations Peacekeeping (2018). https://peacekeeping.un.org/en/how-we-are-funded

[15] BRICS Johannesburg Declaration (2017). http://www.brics2018.org.za/sites/default/files/Documents/JOHANNESBURG%20DECLARATION%20-%2026%20JULY%202018%20as%20at%2007h11.pdf

## Challenges

The foremost challenge for BRICS to be an effective agent of Global Peace and Security is its structure itself. Far from being an alliance, it is not even an organization with a formal treaty or document. In fact, it is this flexibility that has been a positive factor in the evolution of BRICS. It has helped BRICS to adapt to new situations giving the five members enough manoeuvre ability. However, as we saw earlier, in the kinds of security related issues, to move beyond just coordination of positions, one needs a structure and a mechanism particularly if the group is to implement policies.

The second constraint is geo-politics. Each one has its own priorities and considerations. There is no common enemy or adversary. Many of their oppositions are to entrenched principles and concepts which hinder the progress of the emerging countries rather than specific nations.

The third point to be noted is the differing threat perceptions of the five countries. It is only natural because the five are spread across four continents. What may be an existential threat to one may not be considered as serious by the others.

Nonetheless, there are areas which may interest all. That gives hope to meaningful cooperation in this sector.

## Low Hanging Fruits

Given the challenges to cooperation in Peace and Security as mentioned above, BRICS should begin with easily achievable objectives. These can be called low hanging fruits. A gradual and incremental approach would yield the best results. With success in a few initiatives, the credibility of the group in this field would be established leading to tackling bigger challenges.

Some of the low hanging fruits are discussed below.

### *Anti-piracy and Maritime Security*

Piracy is a threat to all nations particularly to those deeply involved in international trade. The incidence of Piracy in the Gulf of Aden along the coast of Somalia has increased over the last two decades. The threat has affected the Arabian Sea also. Many trading nations have had to deal with kidnapping of the crew of cargo ships for ransom. Consequently, all major trading countries like

US, France, China, Japan, Russia, India and South Africa have deployed naval contingents in the Gulf of Aden to tackle the problem. There have also been some coordinated efforts like the ones between India and Japan and India and China. The incidence of piracy in that region has certainly come down. This could also be due to the relative stabilization of the situation in Somalia. Unfortunately, Piracy is not confined to Gulf of Aden. Today, there are more cases of piracy in the Gulf of Guinea near Nigeria through which all the oil exports of West Africa pass. Can BRICS form a mechanism to have joint deployment and joint patrolling? It should not be difficult since the threat affects all of them.

The anti-piracy cooperation can be gradually extended to Ocean Governance in that region. BRICS could become a maritime security provider for the nations on the coasts of the Arabian Sea and the Indian Ocean. There are, however, issues of perceptions of China's increasingly aggressive behavior on the maritime domain to be a leader for providing a global common.

## *Anti-drug and Anti-human Trafficking*

This is another area of common understanding among the five members. Each country has its own program for dealing with these issues. Until recently, there was no coordinated approach. A new BRICS Anti-Drug Working Group has now been set up to deal with narcotics related issues. The group consisting of Heads of Drug Control Agencies of the five countries meets at least once a year to discuss illicit cultivation and production of opium, heroin and cannabis across the globe, illicit financial flows from drug trade and connections between drug trade and terrorism (Josh 2016).

On the question of human trafficking, there has been only modest cooperation so far even though all five realize the seriousness of this crime.

## *Counter-terrorism*

There have been problems with regard to the definition and classification of terrorists. These flow from the geo-political considerations, in so far as the label may be used and applied differently in different parts of hthe world, subject to geo-political alignments.. However, over the last few years cooperation in this field has improved. BRICS have started naming specific terrorist organizations. In the annual meetings of the National Security Advisors (NSAs) of the five countries, counter-terrorism forms a major topic of discussion. This has led to sharing of intelligence and information.

One common understanding of the five on the question of terrorism is their demand for the adoption of a Comprehensive Convention on International Terrorism by the United Nations General assembly (UNGA). The BRICS Declarations never fail to refer to this (Abdenur 2017).

## *Cyber Security*

This is a very new kind of threat faced by all nations. Since regulatory policies always lag behind progress in technologies, governments throughout the world are struggling to keep up with developments in this new threat. There are four broad categories of Cyber Threats: Cyber Warfare, Cyber Espionage, Cyber Crime and Cyberterrorism. Not all governments may be on the same page regarding the definition of and action against the first two; however, nearly everyone is convinced that there should be coordinated international action on Cyber Crime and Cyberterrorism. BRICS is in a good position to come up with some credible solutions.

## *Peacekeeping*

We have seen that the five have a common understanding on some of the fundamental principles of Peacekeeping. How can they leverage this into concrete action? A joint BRICS Peacekeeping Force is, at present, a distant goal. Nonetheless, BRICS could coordinate their existing peacekeeping efforts to avoid duplication and be more productive. Africa, the continent where there are still many conflict areas, could provide an ideal venue for BRICS cooperation. BRICS could contribute resources and personnel towards strengthening the African Standby Force (ASF) and the Rapid Deployment Force (RDF).

## *Non-traditional Security Threats*

Over the past few decades, these have become extremely important in maintaining stability and peace. As is often said, true peace is not just absence of conflicts; it is also absence of those explosive elements, which can lead to conflicts. Many of these elements are in the socio-economic space. They include factors like food security, energy security, livelihood security, a widening gap between the rich and the poor and massive displacements of people. These are catalysts for an eventual crisis, which could explode anytime with a small

incident triggering it. There is need for a constant improvement in the socio-economic conditions of the people. Ensuring that the GINI coefficient (indicating the inequality levels) is within acceptable limits becomes critical.

Having said that, one should not exaggerate the correlation between poverty and inequality on the one hand with terrorism and violence on the other. This narrative could end up in justifying terrorism. After all, global terrorists like Osama bin Laden and Ayman al Zawahiri do not belong to deprived groups. The problem is with the foot soldiers whom they are able to recruit for their acts of terrorism from among the under-privileged. The best example is the Boko Haram group, where, according to some reports, most of the foot soldiers do not necessarily believe in the ideology of the organization, but are in only for the money.

In this context, BRICS could make a more enlightened narrative by going beyond Conflict Resolution to Conflict Prevention. This would require a greater commitment to involving itself in potential crisis areas and dealing with all aspects, particularly the non-traditional threats.

## Governance

It is vital to discuss the role of the governance mechanisms, which are responsible for global peace and security. Governance brings with the principles of vales, norms and rules. It is imperative that we get them right and in the correct sequence. The mechanisms and organizations put in place seventy years ago were products of the victors of the Second World War. With new emerging powers, the scenario has changed drastically. Is it not time the organizations change with changing times to maintain their credibility? To be credible, a global organization needs to be both effective and representative.

The premier agency responsible for global peace and security is the United Nations Security Council (UNSC). The question arises as to how effective and representative is it. It is clear that the present structure of UNSC, particularly the Permanent five with veto powers is no longer in conformity with the current global scenario. Discussions over the last two decades on reforming the UNSC with new emerging powers in the Permanent category have not led to any positive results. Unfortunately, BRICS does not have a common strong position on this question (Abdenur 2017: 79). While two (Russia and China) are Permanent members, the other three are strong contenders for the position as and when there is an expansion. All the Summit Declarations talk about the need for reforming the UN including the Security Council: but they fall short of

recommending the three countries. The maximum that Russia and China say is that they welcome a greater role for the three countries in the UN. Of course, the three are not going to get the Permanent status just because Russia and China say so. It is a long and complicated process where there are other contenders also. Nonetheless, the absence of a BRICS consensus on the subject gives a poor impression about the group. How can BRICS talk authoritatively on issues of global governance when they cannot agree on this crucial question, so as to speak with one voice in the highest form of world security?

## Conclusion

In the last decade, BRICS as a group has achieved considerable heft and influence. It started as a geo-economic group. After a couple of initial Summits, the group began to express its views on geo-political and strategic issues. There was also a coordination of positions on some of the burning problems of the day. The question naturally arose as to whether BRICS can contribute meaningfully to maintenance of Global Peace and Security. There are challenges, the foremost being the fact that BRICS is not a formal alliance. There are also differing geo-political considerations of the five. Nonetheless, there are areas of convergence where they can act together. A positive factor is the agreement of the five to some common principles like the centrality of multilateralism and the UN and opposition to use or threat of force. They also agree on the close interconnection between peace and stability with sustainable development. Due to these factors, it is time for BRICS to undertake some initiatives on Peace and Security. There are many low hanging fruits (as mentioned earlier) which BRICS could achieve first. This would establish the credibility of the group's potential in this activity and lead to further successes. Fear of failure should not deter BRICS from trying out new ideas. The inspiration should be taken from the establishment of the NDB and CRA. Had BRICS been apprehensive of failure at that time, these new institutions could not have been created. The best course of action is to follow a gradual and incremental approach.

BRICS should also utilize the vibrant Track 2 activities to get ideas for peace and security. The BRICS Academic Forum which meets before every Summit and provides useful recommendations to the Leaders as well as the permanent mechanism of the BRICS Think-tank Council (BTTC) are effective platforms to discuss new ideas and come up with practical suggestions. The 10th BRICS Academic Forum, for example, recommended to the Leaders of the 10th

Summit the establishment of a BRICS Peace Research Institute[16]. It could be the knowledge provider for the five governments in the area of Global Peace and Security.

## References

Abdenur, E.A. 2017. Can the BRICS Cooperate in International Security? *International Organisations Research Journal* 12,3: 73 - 91. Available at: https://iorj.hse.ru/data/2017/12/28/1160694810/A.E.%20Abdenur.pdf (Accessed on 04 September 2018.) https://doi.org/10.17323/1996-7845-2017-03-73

BRICS Delhi Declaration 2012. BRICS Partnership for Global Stability, Security, and Prosperity. 29 March. Available at: https://mea.gov.in/bilateral-documents.htm?dtl/19158/Fourth+BRICS+Summit++Delhi+Declaration. (Accessed on 04 September 2018.)

BRICS eThekwini Declaration 2013. BRICS and Africa: Partnership for Development, Integration and Industrialisation. 27 March. Available at: http://www.brics2018.org.za/sites/default/files/documents/eThekwini%20Declaration.pdf. (Accessed on 04 September 2018.)

BRICS Fortaleza Declaration 2014. Inclusive Growth: Sustainable Solutions. 15 July. Available at: http://www.brics2018.org.za/sites/default/files/documents/Fortaleza%20Declaration.pdf. (Accessed on 04 September 2018.)

BRICS Ufa Declaration 2015. BRICS Partnership – A Powerful Factor of Global Development. 9 July, para 8. Available at: http://www.brics.utoronto.ca/docs/150709-ufa-declaration_en.html (Accessed 4 September 2018.)

BRICS Goa Declaration 2016. Building Responsive, Inclusive and Collective Solutions. 16 October. Available at:

[16] Recommendations to the 10th BRICS Leaders' Summit. 2018. 'Envisioning Inclusive Development Through a Socially Responsive Economy'. p.9, 20-31 May, Johannesburg. Available at http://www.nkibrics.ru/ckeditor_assets/attachments/5b3f2a086272690531480000/10th_brics_academic_forum_proposals.pdf?1530866184 (Accessed 11 September 2018).

http://www.brics2018.org.za/sites/default/files/documents/Goa%20Declaration.pdf. (Accessed on 04 September 2018.)

BRICS Xiamen Declaration 2017. BRICS: Stronger Partnership for a Brighter Future. 04 September. Available at: http://www.brics2018.org.za/sites/default/files/Documents/Xiamen%20Declaration.pdf. (Accessed on 05 September 2018.)

BRICS Johannesburg Declaration 2017. BRICS in Africa: Collaboration for Inclusive Growth and Shared Prosperity in the 4th Industrial Revolution. 25 - 27 July. Available at: http://www.brics2018.org.za/sites/default/files/Documents/JOHANNESBURG%20DECLARATION%20-%2026%20JULY%202018%20as%20at%2007h11.pdf (Accessed 7 September 2018.)

BRICS Johannesburg Declaration 2017. BRICS in Africa: Collaboration for Inclusive Growth and Shared Prosperity in the 4th Industrial Revolution. 25 - 27 July, para 52, p.9. Available at: http://www.brics2018.org.za/sites/default/files/Documents/JOHANNESBURG%20DECLARATION%20-%2026%20JULY%202018%20as%20at%2007h11.pdf (Accessed 7 September 2018.)

Contributors to UN Peacekeeping Operations by Country and Post, as of 30 April, 2018. Available at: https://peacekeeping.un.org/sites/default/files/1_summary_of_contributions_2.pdf. (Accessed on 05 September 2018.)

Center for United Nations Peacekeeping (CUNPK) New Delhi, India, 2018. Available at: http://www.claws.in/cunpk.php (Accessed 11 September 2018.)

India and United Nations Peacekeeping and Building 2018. Available at: https://www.pminewyork.org/pdf/menu/49151pkeeping.pdf (Accessed 11 September 2018.)

Jagran, J. 2016. *2nd Anti-drug Working Group meeting of Heads of Drug Control Agencies of BRICS Concluded.* Available at: https://www.jagranjosh.com/current-affairs/2nd-antidrug-working-group-meeting-of-heads-of-drug-control-agencies-of-brics-concluded-1468058264-1 (Accessed 7 September 2018.)

Porto de Souza, F.L. 2015. BRICS: Walking Towards a Common Security Agenda. *Conjuntura Global* 4,2: 133 - 150. https://doi.org/10.5380/cg.v4i2.44233

O'Neill, J. 2001. *Building Better Global Economic BRICS*. Global Economic Paper 66. New York: Goldman Sachs.

Recommendations to the 10th BRICS Leaders' Summit 2018. Envisioning Inclusive Development through a Socially Responsive Economy. 20 - 31 May 2018. Johannesburg. Available at: http://www.nkibrics.ru/ckeditor_assets/attachments/5b3f2a086272690531480000/10th_brics_academic_forum_proposals.pdf?1530866184 (Accessed 11 September 2018.)

Sanya Declaration on BRICS 2011. BRICS Leaders Meeting, Sanya, Hainan, China. 14 April, para 10. Available at: https://www.brics2017.org/English/AboutBRICS/DOPS/201701/t20170114_1116.html (Accessed 4 September 2018.)

United Nations 2015. Transforming our World: The 2030 Agenda for Sustainable Development. United Nations 25 - 27 September 2015. A/RES/70/1, Available at: https://sustainabledevelopment.un.org/post2015/transformingourworld. (Accessed 4 September, 2018.)

United Nations Peacekeeping 2018. *How We are Funded.* Available at: https://peacekeeping.un.org/en/how-we-are-funded (Accessed 7 September 2018.)

H.H.S. Viswanathan
Distinguished Fellow
Observer Research Foundation and
Head: Africa Studies Program
Indian Foreign Service
India
hhsviswanathan@orfonline.org

# Chapter 5: The Menace of Cybercrime, Cyber Security and Regional Response: The Case of Africa

**Isaac Luthuli**

## Abstract

The paper explores the vast, untapped wealth of data and information resources, now worth billions of dollars – and discusses the growing menace of cybercrime and cyber-piracy, which stand as thorns in the flourishing landscape of the digital revolution. 'The momentous digital revolution is facing it's, perhaps, unexpected dimension of physical and cyberspace fraudulent and devastating attacks from cybercriminals. It is estimated that spending on cyber security will escalate from $86.4 billion in 2017 to $93 billion in 2018' (Cybersecurity Ventures 2017). The paper, therefore, cast a glance briefly on the historical landscape on the need to enhance cyber security which started as countermeasure against cybercrimes and its evolving sophistication and complexity. The paper continues to explain the usability and resourcefulness of the cyberspace irrespective of the dangers, which is seen as permanent feature of the digital revolution, and the evolution of digital maturity which is transformation process spurred by the digital revolution in all sectors of businesses. The paper then discusses the trend of cybercrime and cybercriminals' activities globally and in Africa as the spot focus; and citing examples from the main fast growing economic centres on the continent. The study found that Africa potential to grow in the use of internet for various activities, and mostly, in the social media platform and commerce can grow to exceed other parts of the globe that are currently in the lead in terms of internet usage and access. In Africa, the study further discovered the boom (though comparatively low level at this stage) of internet usage for banking, money transfers, ecommerce and social media has been augmented by the mobile telephony. However, safety and protection from cyber-piracy and cybercriminals remain critical, as countless scams, fraud, and incidents of child pornography continue to occur, costing both business institutions such as banks and their

AASBS Volume #21 (2025) https://doi.org/10.29086/978-0-9869938-0-0/2025/AASBS21
Chapter DOI: https://doi.org/10.29086/978-0-9869938-0-0/2025/AASBS21/5 pp. 71 - 100

customers billions in financial losses. Peoples' information infiltration by email spoofing among other forms of cyber-attacks are on the increase found increasing. What options are available? The paper further discusses some policy and legal implications and concluded on the need to find unified and collaboration approach to tackle the menace of cybercrime and cybercriminals remain most tactical cyber security method to mitigate the menace in cyberspace.

**Keywords:** Cybercrime, cyber security, the internet of things (IoT), the case of Africa

## Introduction

The saying that, 'Data is an untapped resource of vast potential that only needs to be unearthed and refined before the riches roll in', remain more futuristic than it is today (Liberty Global Inc.). Thus, the cyberspace appears to be at the beginner stage of something earth-shattering, and we are yet to drive into the real arena of the digital era and what it actually entails to advance humankind into a utopian dream or something obnoxious. It is estimated that 'cybersecurity spending will grow from $86.4 billion in 2017 to $93 billion in 2018' (Cybersecurity Ventures 2017). But whichever direction to drive the digital paradigm is a choice humanity has to make today for the best or for the worst must come out of collaborative global policies that tackles and deal firmly with evil onslaught on the digital super highway. Though some of us were born in the internet era which makes it something normal, it is still an amazing feat for humanity to be able to use the digital technology from approximately the last of the twentieth Century to create a global village, and possibly, an inter-planetary networking. Today, we can be thousands of kilometre apart but next to each other chatting, browsing, trading, conferencing, receiving medical treatments, weather surveillance, researches, military purposes, safety monitoring, money transfers and banking, sourcing information of all kinds just within few minutes, space exploration and many other values internet and digital revolution has brought humanity. Yet it is the same technology that has become a menace to the global community, as cybercrime and cybercriminals are increasing every minute and the need for cyber security has become critically important and crucial with the amorphous nature of cybercrimes and cybercriminals. Cyber security is defined as a 'set of activities, technical and non-technical aspects of protecting information, devices, computer resources, network resources and other critical information stored therein from unauthorized

access, modification and disruption, disclosure' (Verma & Sharma 2014). So, indeed, humanity have got such a blessed rose - the internet, but not without the torn, as the cyberspace has become an arena of extreme and wide scale damning fraudulent and destructive activities. The internet value also opens studies in Information Technology and wider growing market absorbing people with skills in internet related jobs. Today also there are state departments created for IT which oversee the usage and control of internet activities. This paper, thus in discussing cyber security situation of the present will do so by looking at these sub-themes: The Internet of Things as the Centre of Global Interactions; Critical Cybercrime Target Areas and Cyber Attacks Today; Cyber Security and Managing Cyberspace Risks; Policy and Legal Concerns; Recommendations; and Conclusion.

## The Internet of Things as the Centre of Global Interactions

### *Brief Backgrounds*

We begin with some glimpse of background to the situation of cybercrime. As computer use mainly in big institutions and not of commercial value yet, computer crimes started on 'offences focused on physical damage to computer systems and stored data' in the 1960s. Such crimes were prevalent in the West, especially USA, Canada and Europe. In the 1970s the growth in Computer systems and usage - automation or computer-operated transactions led also to emerge new forms of computer crimes including computer-related fraud as the 'illegal use of computer systems and the manipulation of electronic data' (Gercke 2012). That compelled the USA Government to come up with bill 'designed specifically to address cybercrime' (Gercke 2012). Also the matter was then taken up by the Interpol concerning 'the phenomena and possibilities for legal response' (Gercke 2012). As commercial and personal computers entered the market of the emerged digital era and cellphones outdoor in the 1980s, Western Governments got concerned on legal matters regarding growing related cybercrimes. Indeed, the enormity of the situation made 'OECD and the Council of Europe set up study groups to analyse the phenomena and evaluate possibilities for legal response' (Gercke 2012).

By the end of the twentieth century and the dawn of the World Wide Web (www), which linked the entire Earth into just a cyberspace with all its comprehensive benefits, became highly vulnerable to full-blown activities of computer crimes that translated into cybercrimes. Thus, among other legal measures to curb and deal with cybercrimes by some countries, the UN General Assembly Resolution 45/121 which was adopted in 1990 and made a manual for

the prevention and control of computer-related crimes in 1994 (Gercke 2012). According to the ITU 2012 Report (compiled by Marco Gercke), 'The first decade of the new millennium was dominated by new, highly sophisticated methods of committing crimes, such as 'phishing', and 'botnet attacks', and the emerging use of technology that is more difficult for law enforcement to handle and investigate, such as 'voice-over-IP (VoIP) communication' and 'cloud computing'. Hence, the menace of cybercrime as unprecedented and with much unknown concerning its perverting insidious activities, is more or less a permanent feature of the digital era which requires dynamic responses.

## *The Importance of the Internet for Humanity and its Continuing Advancements*

The growth of the internet and its expansion, thus, sprawling to almost every facet of living to business transaction, education, health and among others is not only captivating, but it will continue to transcend the present scope of usability and versatility. As at 2016 the population estimate of users was approximately over three billion (3.4 billion) which represents forty-six percent (46%) of global population (Internet Life Stats 2026). Today, some companies have switched to full-automation using digital technology that is computer or robot based. Several other companies globally are following that initiatives and investing in digital.

For example, traditional human labour-based mining is shifting to digital operations using computers and robotic automatons in Australia and Canada, etc. In Africa some mines in Democratic Republic of Congo (DRC) are being operated by robots cutting on human labour and the risk involved (https://phys.org/news/2018-03-cobalt-boom-life-upside-dr.amp).

Some aspects of South African mines, manufacturing sector, automotive industries, and agricultural sector have partially been automated and these automatons can be hacked with current development in cybercrime (Rojanasakul & Peter Coy 2017).

## *Evolution of Digital Maturity*

The emerged digital paradigm and its growth has come with classification of organisations, companies and industries into levels of 'digital maturity'. The term comes with two dimensions which describe and determine companies' levels of innovation in line with the digital revolution. The first dimension is 'digital

intensity, is investment in technology-enabled initiatives to change how the company operates – its 'paradigm shift from a company centric logic to a customer engagements, internal operations, and even business models' (MIT Center for Digital Business, undated). The trend comes up with consumer-centric logic'[1].

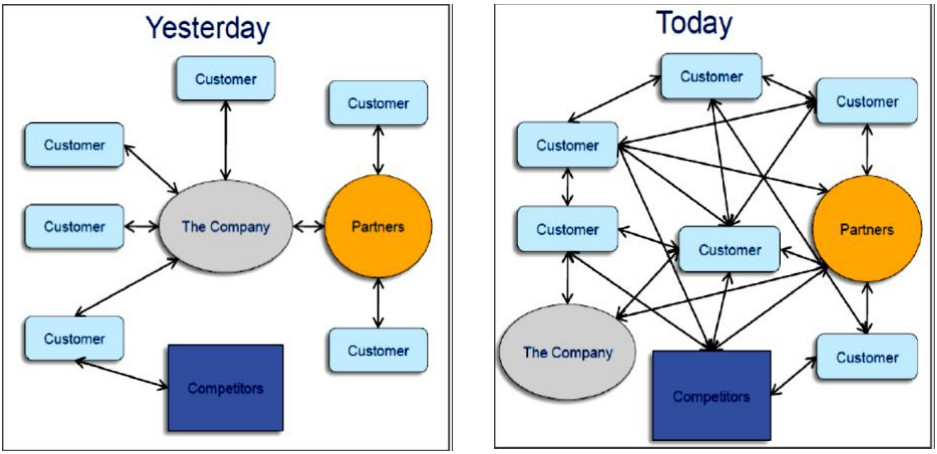



**Figure 1. A shift from Company-centric to consumer-centric logic**
**Source: Dervojeda, Kristina *et al.* (2014)**

The second dimension is 'transformation management intensity'. That involves 'creating the leadership capabilities necessary to drive digital transformation in the organization. Transformation intensity consists of the vision to shape a new future, governance and engagement to steer the course, and IT/business relationships to implement technology-based change'. So, there are several organisation, companies and industries that have embarked on full maturity drive and others that remain unconvinced on such move based on management stereotype and perceived fear of transformation in the digital drive and sphere.

[1] Dervojeda, Kristina *et al.* 2014. *Innovative Business Models for Competitiveness: Social Media for Internationalisation*. Business Innovation Observatory. Contract No 190/PP/ENT/CIP/12/C/N03C01. Available at: http://ec.europa.eu/enterprise/policies/innovation/policy/business-innovation-observatory/files/case-studies/22-ibm-social-media-for-internationalisation_en.pdf

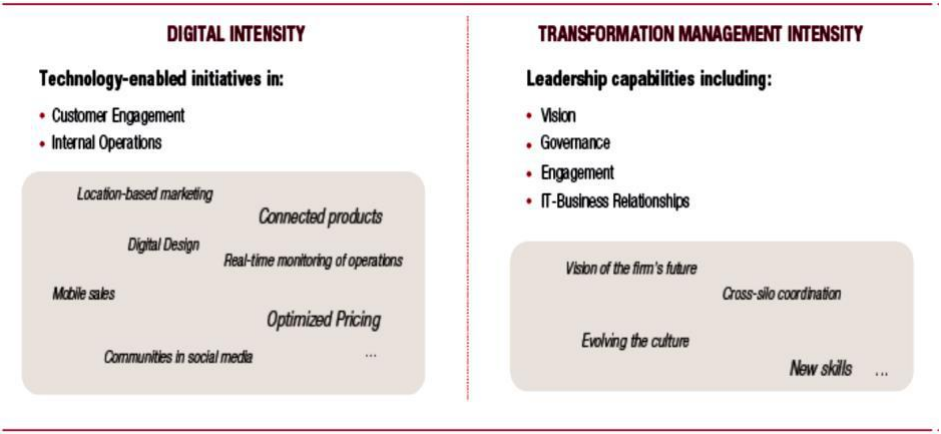



**Figure 2. The What-and-How of Digital Transformation – Two Dimensions of Digital Intensity**

Most of the digital matured entities have implemented technology-based change to build digital innovations, and to drive enterprise-wide transformation, and they benefit from their actions which are yielding results of efficiency and effectiveness (MIT Center for Digital Business, undated). However, despite using digital or automated technology to replace humans not only for efficiency and effectiveness but eliminating certain high-level risks, the aspect of risk as result of cybercrime has become even more serious.

The fact is that digitalizing and digital innovations are generally internet based and computer or robot based. This also has been termed the Internet of Things (IOT) (Dawson 2017). According to SAGE Group the Internet of Things (IoT) describes 'the ever-growing network of "things" – objects embedded with unique identifiers that are able to transfer data over a network without human involvement' (The SAGE Group 2017). The ability to connect in network at fast speeds also comes with implications of being hacked. Despite the dangers pose by interconnectivity the benefits of cyberspace far outweigh the crimes that have infiltrated the space. It is known that in commercial value 'there is a potential market that approximately $14.4 trillion and over 99 percent of physical devices are still unconnected' (Dawson 2017).

## Critical Cybercrime Target Areas and Cyber Attacks Today

### *The Menace of Cybercrime*

Reddy and Reddy (undated) explain that according to WiseGeek cybercrimes are 'any type of illegal activity that makes use of the Internet, a private or public network, or an in-house computer system. While many forms of cybercrime revolve around the appropriation of proprietary information for unauthorized use, other examples are focused more on an invasion of privacy (Reddy & Reddy, undated)'[2]. Wikipedia defines computer crime, or cybercrime as 'any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target …. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise'[3].

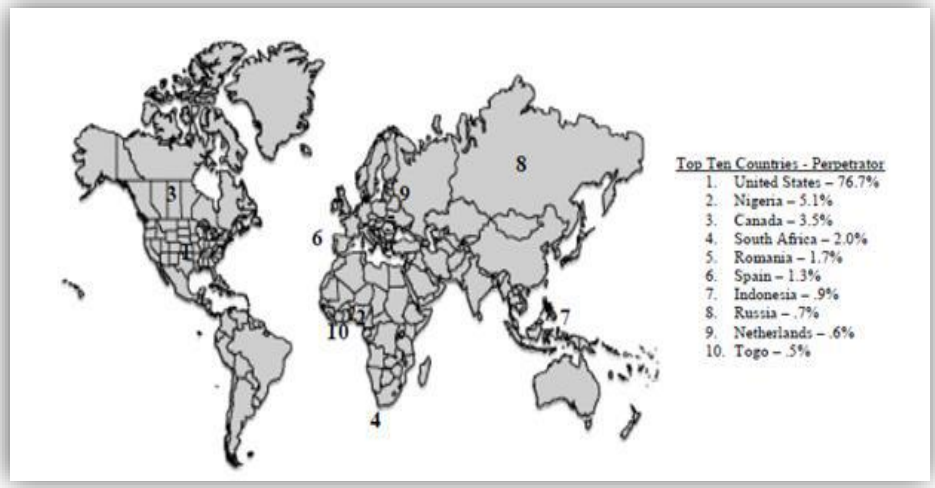



**Figure 3. Top 10 states and country perpetrators - IC3 reports**

The usability and usefulness of the cyberspace is its command of extreme capacity in 'the importance – and value – of data' storage and retrieval (Liberty Global Inc.). A document by Sloans describe the value of pool of data currently generated and stored in digital form as 'the new gold'. Francis Maude, the UK

[2] See also: http://www.wisegeek.com/what-is-cybercrime.htm
[3] See also: http://en.wikipedia.org/wiki/Computer_crime

Minister for the Cabinet Office also describes the cyber world of data as the 'new raw material of the 21st century'. The cyberspace has such gigantic capacity to capture data of entire galaxy and still room to take on more and that is the unlimitedness of the digital world. Thus, the cyberspace is by and large information based and therefore carries the threat of invasion and the need to secure information from being accessed unwarranted and abused for various diabolical purposes. Personal information has been input on various database of multitude of organisations, companies, institutions and state departments. Liberty Global Inc. (2012), publication raise the issue of 'our digital identity' defined as 'all the bits and pieces of information about us that are readily, and increasingly, available in digital form; data that is collected and analysed to create a surprisingly accurate, and ever-improving, picture of who we are, what we do, what we like (and what we dislike, too)'. So digital identity has become a major digital pool for marketing and tracking potential clients and customers globally.

The European Commissioner for Justice Viviane Reding said in Janu-ary 2012, when presenting the proposal for the new General Data Protection Regulation, 'Personal data is in today's world the currency of the digital market' (Liberty Global Inc. 2012). The implication has been that as much as 'currency can be volatile, so and personal data is no exception' (Liberty Global Inc. 2012). Thus, the issue about privacy and how best organisations storing digital identities can ensure safety and not being breaching through activities of hackers re-main contentious debate. There is ongoing hacking of some companies and social media database where members' information has been stolen. The Face-book has suffered such attacks (Liberty Global Inc. 2012). But it indisputable that consumers and society cannot avoid submitting digital identity to organisations most importantly banks, insurance firms, state departments and many more. So, the matter come to rest on how best to ensure secured security and means to anticipate the hackers' innovations and dexterity? This will be answer-ed in subsequent section on Cyber security. What we want to look at next is the nature of cybercrime and the rationale for most of the ongoing cybercrimes.

## *Types of Cybercrime Offences*

i. Offences against the confidentiality, integrity and availability of computer data and systems;
ii. Computer-related offences;
iii. Content-related offences; and
iv. copyright-related offence (Paryag & Griffin, undated).

## *Causes of Cybercrimes and Techniques Employed*

- **Hacking:** In other words can be referred to as the unauthorized access to any computer systems or network. This method can occur if computer hardware and software has any weaknesses which can be infiltrated if such hardware or software has a lack in patching, security control, configuration or poor password choice.

- **Theft of information contained in electronic form:** This type of method occur when information stored in computer systems are infiltrated and are altered or physically being seized via hard disks; removable storage media or other virtual medium.

- **Email bombing:** This is another form of internet misuse where individuals directs amass numbers of mail to the victim or an address in attempt to overflow the mailbox, which may be an individual or a company or even mail servers there by ultimately resulting into crashing. There are two methods of perpetrating an email bomb which include mass mailing and list linking.

- **Data diddling:** Is the changing of data before or during an intrusion into the computer system. This kind of an occurrence involves moving raw data just before a computer can processes it and then altering it back after the processing is completed.

- **Salami attacks:** This kind of crime is normally consisting of a number of smaller data security attacks together end resulting in one major attack. This method normally takes place in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. This form of cybercrime is very common in banks where employees can steal small amount and it is very difficult to detect or trace an example is the 'Ziegler case' wherein a logic bomb penetrated the bank's system, which deducted only 10 cents from every account and deposited it in one particular account which is known as the 'penny shaving'.

- **Denial of service attack:** Is basically where a computer system becomes unavailable to its authorize end-user. This form of attack generally relates to computer networks where the computer of the victim is submerged with more

requests than it can handle which in turn causing the pc to crash. E.g. Amazon, Yahoo. Other incident occurs November 2010 whistle blower site wikileaks.org got a DDoS attack.

- **Virus/ worm attacks:** Viruses are programs that can embed themselves to any file. The program then copies itself and spreads to other computers on a network which they affect anything on them, either by changing or erasing it. However, worms are not like viruses, they do not need the host to attach themselves to but make useful copies of them and do this constantly till they consume up all the available space on a computer's memory. E.g. love bug virus, which affected at least 5 % of the computers around the world.

- **Logic bombs:** They are basically a set of instructions where can be secretly be execute into a program where if a particular condition is true can be carried out the end result usually ends with harmful effects. This suggests that these programs are produced to do something only when a specific event (known as a trigger event) occurs. E.g. Chernobyl virus.

- **Trojan attacks:** The term suggests where a program or programs mask themselves as valuable tools but accomplish damaging tasks to the computer. These programs are unlawful which flaccidly gains control over another's system by assuming the role as an authorised program. The most common form of a Trojan is through e-mail.

- **Internet time thefts:** This form is kinds of embezzlements where the fraudulent uses the Internet surfing hours of the victim as their own which can be complete by obtaining access to the login ID and the password.

- **Web jacking:** This is where the hacker obtains access and can control web site of another person, where he or she can destroy or alter the information on the site as they see fit to them. This type of method of cybercrime is done for satisfying political agendas or for purely monetary means. An example of such method was MIT (Ministry of Information Technology) was hacked by the Pakistani hackers whereas another was the 'gold fish' case, site was hacked and the information relating to gold fish was altered and the sum of $1 million was demanded (Paryag & Griffin – undated). http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

## *The Motives behind Cyber Attacks – Revenge to Notoriety*

The table below comes with few of the most common factors and rationale.

| Why They Do It – What are the Motives? | Cyber attackers to Law Enforcement entities | Cyber Vulnerabilities of Law Enforcement Agencies |
|---|---|---|
| • Disabling Websites<br>• Public Exposure of the Private Information<br>• Espionage<br>• Interference with Police Operations and Sabotage<br>• Defacing to Cause Embarrassment or Retaliation<br>• Retribution<br>• Profit<br>• Notoriety<br>• Disinformation | • Hacktivists<br>• State Actors<br>• Criminal Organizations<br>• Terrorist Organizations<br>• Purposeful or Accidental Insider<br>• Individuals | • Personnel<br>• Organizational Barriers<br>• Information Networks & Systems<br>• Public-Facing Websites<br>• Data Storage Devices<br>• Social Media Accounts<br>• Communications Centers, Systems, Equipment and Applications<br>• Wireless Devices<br>• Facility Systems and Physical Infrastructure |

The commonality of cybercrime has got to the stage creating uncontrollable vulnerability for many organisations, companies and institutions that 'an employee clicking on a macro within an email which in turn downloads a pro-gram, which then automatically pulls down targeted malware to access network resources (this is sometimes known as 'weaponised email attachments')' Australian Computer Society 2016). And as the cyberspace has become the digital office, market and trading place, banking business, research space, health and treatment consulting, forums and legislature arena to almost everything, such vulnerability must be considered as critical and alarming for much effective actions to secure the safety of internet usage which actually is not reversible. The nature of attacks as shown varies and continue to extend into new targets and evidences show that 'attacks can serve several purposes including fraud, extortion, data theft, revenge or simply the challenge of penetrating a system', and some of the cybercrimes or cyber-attacks 'can be done by internal employees who abuse

their access permissions, or by external attackers to remotely access or intercept network traffic' (Yassir & Nayak 2012).

## *Cybercrime Trends in First Quarter of 2018*

Q1 2018 represented the largest ever digital quarter for the ThreatMetrix Digital Identity Network:

- ✓ 210 million attacks were detected and stopped in real time; a 62% increase over the previous year.
- ✓ In addition, the risk landscape has heightened: attack growth outpaced transaction growth by 83% in comparison to Q1 2016.
- ✓ This quarter has seen a proliferation of attacks on the eCommerce industry: eCommerce transactions are now more than 10 times riskier than those in financial services, highlighting the fact that cybercriminals see eCommerce as a growing target.
- ✓ Organized bot attacks continue to proliferate, with a record 1B bot attacks seen in the Network this quarter, 100M of which were from mobile devices. These bots are predominantly targeting eCommerce merchants.
- ✓ The anatomy of bot attacks continues to shift and morph; transactions from several new and emerging economies such as Vietnam, Egypt, South Korea, Ecuador and Ukraine are very likely to be bots, and contribute significantly to the overall bot volumes seen globally.
- ✓ 51% of transactions in the Network come from mobile devices (55% for financial institutions), a 170% increase compared to Q1 2015.
- ✓ 60% of all account creations are now done on a mobile device, indicating the increased role of mobile as the key enabler across the entire customer journey.
- ✓ However, many consumers still perform large / complicated actions across a range of devices, indicating the need for businesses to look beyond device intelligence to verify identity and authenticate transactions.

(ThreatMetrix Digital Identity Network 2018)

## *Global Trends*

As the internet generally and largely is all about information and an aspect of that have been identified as digital identity. That encourages regular daily rate of attacks on consumers and users of the internet facilities. Figure 4. shows that the daily attack of graph patterns from 2015 to 2018 first quarters depict unpredictability of attacks and varies with intensities.

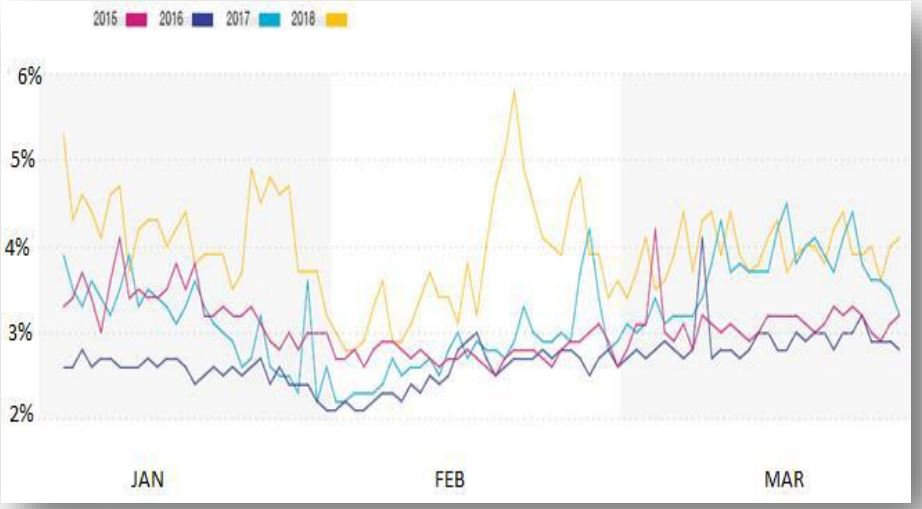



**Figure 4. Q1 Daily Attack Rate 2015 to 2018**
**Source: 2018 CYBERCRIME REPORT - (ThreatMetrix Digital Identity Network 2018)[4]**

The major concern of all types of digital information apart from those that are made public without restriction is about their security of data.

[4] Attack percentages are based on transactions identified as high-risk and classified as attacks, by use case. Events identified as attacks are typically blocked or rejected automatically and in real time depending on individual customer use cases (Quoted).

That comes with the need for cyber security to ensure information that are restricted are secured according to guarantees; and people's digital identity and other information are not abused and taken advantage of by hackers. The reason is estimates shows that 'the number of IoT devices will be three times as high as the global population by 2021' (Cited in Cybersecurity Ventures 2017). Also, for growth of cell phones see, Dervojeda *et al.* 2014). Pahi, Leitner and Skopik (2017) have expressed the concern that **'**critical infrastructures, personal identity, important fiscal information and trade a secrets, proprietary information and the customers' information must to be a safeguard against as a possible cyber-attacks'.

In view of that the solution as they observed lies in 'Cyber security standard' that must be continually developed to reduce the risk of cyber-attacks effects and impacts. That calls for collaboration approach at governmental and inter-governmental levels with the private sector on Public Private Partnership (PPP) to achieve standards that outrank the dexterity and smartness of cyber-attacks and cyber criminals.

Concerning information available on the internet, there are varied information which are organized into four main categories which are namely. These are organised in the figure 5. below.

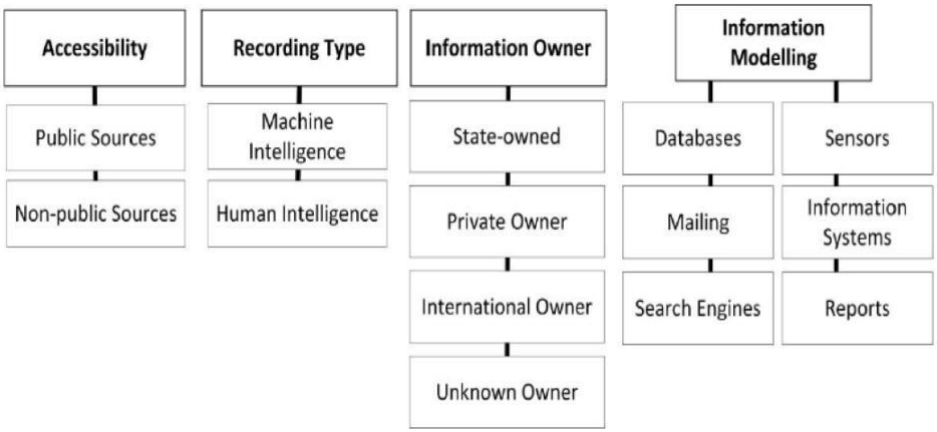



**Figure 5. Categorization of information sources. Source: Pahi *et al*. (2017)**

**In summary, the five types are:**

- Accessibility types which consists of public sources and non-public sources information;
- Recording type which consists of machine intelligence and human intelligence;
- Information owner category that consists of state-ownership, private ownership, international ownership and some other unknown or disclaimed ownership; and
- Information modelling category which consists of two parallel streams with the first forming databases, mailing and search engines; and second stream forming sensors, information systems, and reports.

Information can also be categorized under digital volumes from megabytes to gigabytes and terabytes. There are various information interface platforms which help in determining the content levels and capacity under which to place such content information.

Figure 6. below portrays the levels of cyber interface platforms and their volumes or capacities with all of them involving capture and storage of digital identities.

From the 1990s to 2015 digital services and media ranked lowest in volume space of $4.97 \times 10^5$ TB. Online transactions since 2000 when such activities grew for example databases and trade flow trends, Google search engine ranked third in cyberspace volume. The IOT 2003 ranked second occupier of cyberspace volume; and the commencement of social media from 2007 to 2015 ranked highest with Facebook, Twitter, YouTube and many others have massive digital identities.

Today these figures have grown within the last three years, but still maintainthe same ranking positions. The overall information volume is rising every second at tremendous rate. However, the security concerns remain critically nebulous and left in the hands of individual countries when the cyberspace remain grossly borderless and mainly uncensored.

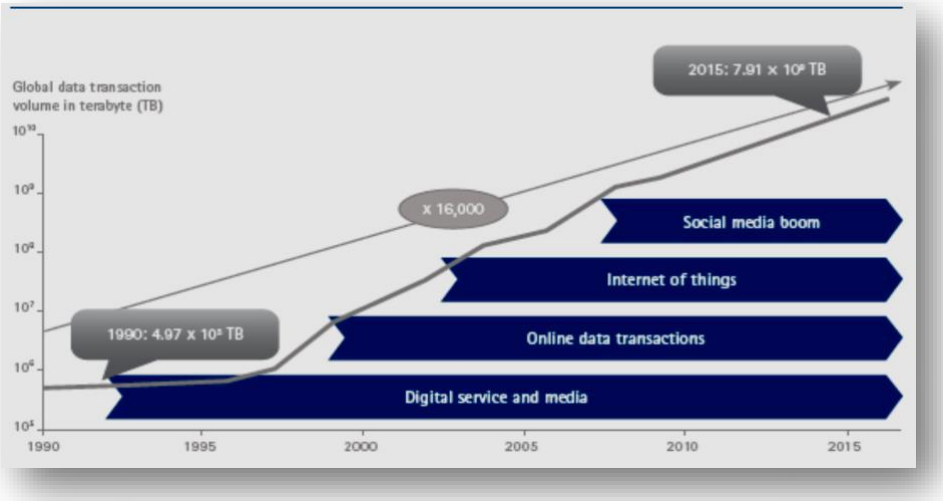



**Figure 6. Source: comScore; Facebook; Sandvine: 'Information White Paper' 2011; Sandvine: 'Digital Contents White Paper' 2010; METI E-Commerce survey; IDC; consumer research; BCG analysis**

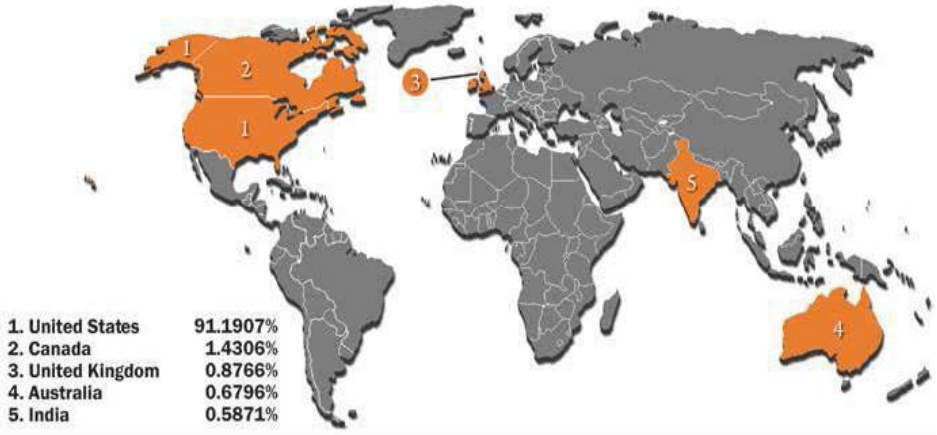



**Figure 7. Top 5 Countries by Count: Victim Complainants (Numbered by Rank) 2012. Source FBI quoted in Verma and Sharma 201**

Figure 7. shows the top 5 countries that have the most cyber-attack complaints. Only few countries like China and North Korea censor the internet and restrict access on certain platforms especially social media and news media but such restrictions do not prevent cyber-attacks. As the cyberspace has become information gold mine and at the same vulnerable to cyber-attacks, espionage and hackings makes the public feel insecure on the amount of personal data out there in the cyberspace. Organisations' secrets sit vulnerably on their computers and military information and installations have come under severe attacks in inter-state cyber warfare, especially between America and Russia (Baylon 2014; Australian Computer Society 2016). In 2016 US Democrats Presidential Candidate Hillary Clinton was beaten by her rival Donald Trump with her defeat being attributed to Russia hacking her personal emails and exposing certain information that weakened her possibility of winning. The ongoing investigation have been refuted by Russia as untrue but obviously that is how inter-state espionage and cyber warfare works – attacks and denial. In South Africa concerns have been drawn to how a website was able to access National Department of Home Affairs (NDOHA) database and exposed national identity information of citizens and permanent residents in South Africa.

## *Healthcare Industry Security Threats*

The health sector has become one of the most critical target of cyber-attacks and hackings. The latter is used to steal data of clients and used for wrong purposes. Experts are concerned how cyber-attack can infiltrate health system and alter sensitive information that can cause harm to users. According to Alharam and El-madany (2017) 'Healthcare applications are very critical applications and medical data are very critical and complex to be secure than other type of data and applications because it needs to be highly secured …. security threats are eavesdropping, impersonation, message modification, and Man-in-the middle'. Cybersecurity Ventures Group (2017) have painted much grim picture that 'Hundreds of thousands – and possibly millions – of people can be hacked now via their wirelessly connected and digitally monitored implantable medical devices (IMDs) – which include cardioverter defibrillators (ICD), pacemakers, deep brain neurostimulators, insulin pumps, ear tubes, and more'. Because of the foreseen risk and danger healthcare provider are investing in much modern cyber security systems to protect their infrastructures and patient data, especially from

2017. Furthermore, with the development of online treatment using social media platforms and mobile phones, the need to ensure clients are not caught in the net of cyber criminals is important and how to authenticate service providers from spoofing.

## *Artificial Intelligence Control Systems and Facilities*

These are categories of computer based control systems used for high task demands like aviation traffic controlling, railways controlling, weather monitoring, pest controlling, tracking systems, commercial satellites, power distribution systems, military installations for security purposes, automated operations system controlling and some others remain vulnerable these days with cases of interceptions and interferences that 'can affect the function and reliability of services in many different segments of the orbital infrastructure, i.e. broadcasting, communication links, navigation and positioning, and civilian Earth observation' (Jolly 2014).

## *Scenario in Africa*

Africa remains the continent with little internet penetration though the mobile phone revolution has helped achieve the level so far. It is estimated that 'revenues from mobile telephony now represent 3,7 % of GDP on the African continent - a ratio three times higher than in developed economies' (Shiloh & Fassassi 2016). The connectivity of mobile phones enable all kinds of activities from social media to e-commerce.

In 2014 Dervojeda, Kristina *et al.* (2014) forecasted that 'Although Asia-Pacific will have the largest social network population worldwide through 2017, and the Middle East and Africa will have the second-largest audience …, their population penetration rates are still among the lowest.

This means that growth potential for social media, and marketing based on it, is huge', caused by growth in the use mobile telephony in particular, to transact on internet (Dervojeda *et al.* 2014). But the question remains how much secure are people with the internet penetration in Africa if even those in the technologically advanced countries are facing serious cyber-crimes?

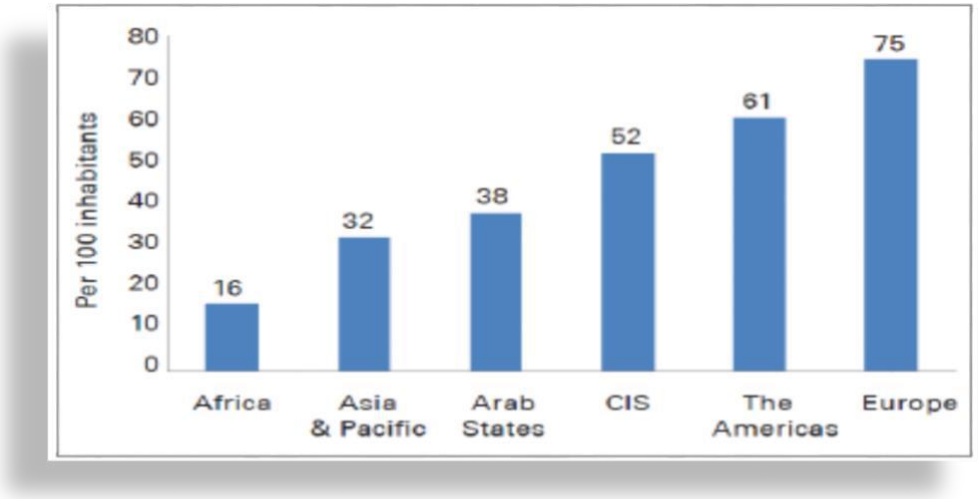



**Figure 8. Diffusion of internet across the world. Source: Dervojeda *et al.* 2014.**

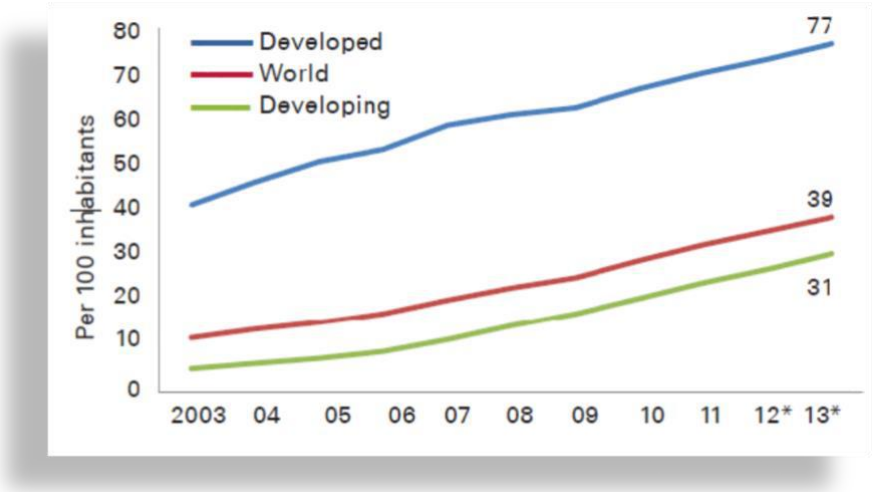



**Figure 9. Diffusion of internet across the world.**
**ITU World Telecommunication/ICT indicators database captured from Dervojeda *et al.* (2014). Note: * Estimate**

Evidences available show not surprisingly as such, the onslaught of cybercriminals on the continent's most active economies (figure 10). According to Serianu (2018) 'Estimated cost of cyber-crime in Africa has soared as follows, Nigeria ($550 million), Kenya ($175 million), Tanzania ($85 million), Ghana ($50 million) and Uganda ($35 million) Cost of Cybercrime $895m'. Dawson, Lieble and Adeboje (undated) have pointed out that 'Nigeria is Africa's largest economy surpassing South Africa in recent years. However, this country is home to the infamous 419 Scam in which gained international attention due to the number of individuals this scam has taken financial advantage of globally'.

| | Population (2016 Est.) | GDP (2016) | Internet users & subscribers (2016) | Estimated Cost of cyber-crime (2016) | Estimated No. of Certified Professionals |
|---|---|---|---|---|---|
| Africa | 1,185,529,578 | $2.89T | 340,783,342 | $2B | 6892 |
| Nigeria | 186,879,760 | $481.066B | 97,210,000 | $550M | 1500 |
| Kenya | 46,790,758 | $63.398B | 37,716,579 | $175M | 1400 |
| Tanzania | 52,482,726 | $44.895B | 17,263,523 | $85M | 250 |
| Ghana | 26,908,262 | $37.86 B | 19,125,469 | $50M | 460 |
| Uganda | 38,319,241 | $26.369B | 14,564,660 | $35M | 300 |

**Figure 10. Breakdown of key statistics for In-Scope countries. Source: Serianu AFRICA CYBER SECURITY Report**

The scope of malicious cyber activities in Africa covers malware, attacks, spam, phishing hosts, bolts, and C&C servers (Symantec Telemetry) (Yedaly & Wright 2016) (figure 11).

The figure 12, shows the most susceptible countries in Africa currently ranked as top 10 countries on the continent for attacks. South Africa tops the 10 top countries for cyber-attacks of all kinds with likelihood of 31 percent with incident count of 220, 727. It is followed by Morocco, Uganda, Egypt, Mauritius, Kenya, Tunisia, Nigeria, Zimbabwe, and Algeria.

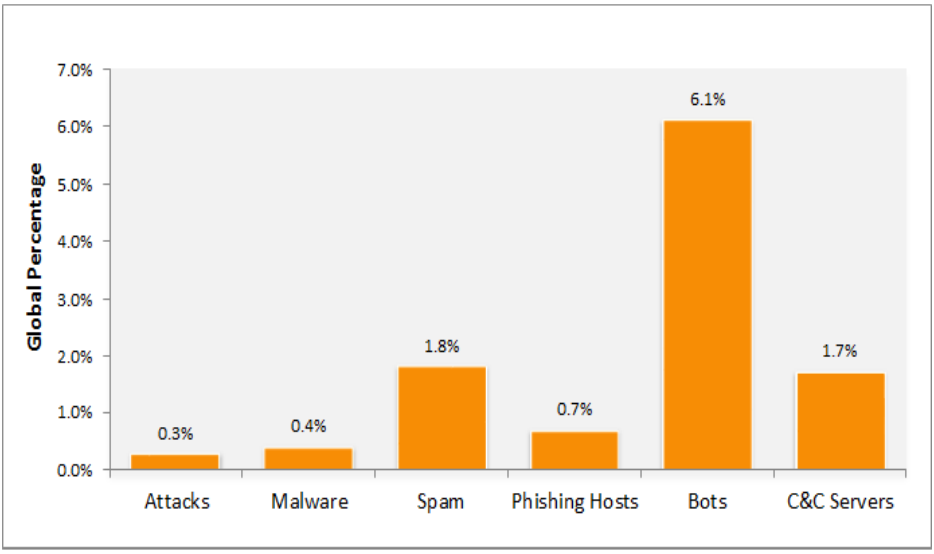



**Figure 11. Malicious Activity Originating from Africa**

There are further reports revealing that 'Business email scams led to losses amounting to USD 2 million in the African region in 2016. Majority of these emails affected organisations that conduct international business and targeted financial managers who were instructed by their 'CEO' to transfer money to foreign accounts' (Serianu Ltd 2016).

| Country | Africa Rank | Percentage | Incident Count |
|---|---|---|---|
| South Africa | 1 | 31% | 220,727 |
| Morocco | 2 | 16% | 106,144 |
| Uganda | 3 | 10% | 63,234 |
| Egypt | 4 | 9% | 57,204 |
| Mauritius | 5 | 8% | 52,974 |
| Kenya | 6 | 4% | 27,172 |
| Tunisia | 7 | 4% | 25,665 |

| | | | |
|---|---|---|---|
| Nigeria | 8 | 3% | 20,158 |
| Zimbabwe | 9 | 3% | 19,319 |
| Algeria | 10 | 2% | 10,790 |

**Figure 12. Top 10 source African countries for attacks**

The main factor is not developing country matter where lack of skills can be an issue but cybercrime is international and complex that there is need for both regional and global cooperation. Further reports also shows 'several Zambian commercial banks were defrauded of over 4 million dollars in the first semester of 2013, as a result of a complex cybercrime scheme involving Zambians as well as foreign nationals' (Shiloh & Fassassi 2016).

In Ivory Coast '1.409 complaints had been lodged and acted on by the Ivorian courts last year. According to him, the global volume of Web based fraud in the country seems to have started to decrease, falling from 5.8 billion CFA francs (8.9 million euros) in 2014 to 4 billion CFA francs (6, 1 billion euros) in 2015' according Charles Kouamé in charge of governance in the Ivorian Authority for the regulation of telecommunications giving a report at an international forum on cybercrime in 2016 in Dakar (Shiloh & Fassassi 2016).

In South Africa 3 Nigerian nationals Oladimeji Seun Ayelotan, 30, Rasaq Aderoju Raheem, 31 and Femi Alexander Mewase, 45, were tried in USA Southern District of Mississippi after extradition and convicted of wide-ranging internet fraud schemes (romance scams, re-shipping scams, fraudulent cheques scams, working-at-home scams as well as bank, financial, and credit card account takeovers) in a United States court, unravelling a large network of international internet scammers (Singh 2017 – News24). South Africa Police cybercrime unit have been working actively on cybercrimes and criminals understanding the complexity of the matter. Cases of child pornography outlawed in South Africa and Africa are monitored in collaboration with overseas security interceptors (O'Reilly 2008).

## *Next Innovations*

There are several researches and innovations yet to be produced on commercial scale which are robotic and susceptible to cybercriminals interferences and attacks. For example, 'traffic authorities see nearly 300,000 lives saved over the

next 10 years from a vast reduction in traffic fatalities using autonomous vehicle technology' (Cybersecurity Ventures 2017). In 2017 a collision prevention automotive technology developed by Mobileye, an Israeli have been acquired by Intel at $15.3 billion to be installed on nearly 15 million vehicles. New intelligent and cutting-edge home security remote monitoring sensors and metropolitan sensors coming out is expected to cut down crime levels by 20 percent (Cybersecurity Ventures 2017).

## Cyber Security and Managing Cyberspace Risks

### *Current Cyber Security Developments*

The case remain that to combat and mitigate cybercrimes requires effective policies crafted work across borders. The need for other supportive monitoring private entities that feed into the Interpol have also emerged. In fact, most of the information used come from private entities engaged in monitoring the cyberspace activities. These are aspects of cyber security as security strategy matter to counteract all the tactics of cybercrime and cyber criminals. Furthermore, experts believe 'cyber security plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being' (Yadav *et al.* 2013). A survey conducted by Cisco found that 40 percent of the manufacturing security professionals responding to a recent Cisco survey said they do not have a formal security strategy' (Cybersecurity Ventures 2017). There are technical and institutional challenges facing effective cyber security strategy. Hence experts' opinion points to taking steps to wield 'coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation' (Gercke 2012). The critical challenge is the fast-growing cybercrime rate has implications for rising cost of cyber security strategy planning and execution, because of growing increase in IOT devices and connections to the network (Cybersecurity Ventures 2017).

### *Policy and Legal Concerns*

#### *Legal*

The legal connotations cannot vary too much as the cyber space link all countries into one global unit. In that case we find criminal transactions are operated across countries as the case of Nigerians operating from South Africa to do cyber heist

in the USA and elsewhere. The root sources differ from the crime spots and very complex maze of criminal activities based on cyberspace is fast developed into multibillion money laundering activity. The need to have uniform and common laws or legal framework that can be fast applied without boundaries issues is essential. If one state's legal system makes it difficult to pursue cybercriminals, which could jeopardize the entire global oversight without appropriate institutions of states and private sector collaborations and involvement. In South African Government Cybercrimes Bill, for example, was passed in December 2017 that aims to eliminate the challenge of cyber criminality (Department of Justice and Correctional Services – Republic of South Africa 2016). The success of that Bill has seen child pornography criminals who market their criminal products using the internet.

## *Technical*

At the technical level the onerous challenge remain strategic. The need to outpace cybercriminals and their growing networks and dexterity. That requires the development of technical solutions that are cost effective and efficiency taken into consideration. As much as cybercrime can be considered a permanent face of reliance on internet as cyberspace and cyber-technologies and devices, humanity today will not only have the task of fighting disease but actively fighting and dealing with cybercrimes and cyber criminals too.

## *Institutional*

There are various institutional measures working with examples being:

i. Electronic Commerce by the United Nations Commission on Trade Law

ii. The UN Office on Drugs and Crime (UNODC). This organisation has mandate that focuses on cybercrime and its law enforcement applications, especially across boundaries.

iii. It oversees the publicizing the tenets of the Budapest Convention on Cybercrime and capacity-building on cybercrime issues at the national and regional levels.

iv. For most member states of the UN the issue of cyber security is a serious,

recognized threat economically and politically. The notable WikiLeaks have damning implication for geopolitics as case example where emails and cable messages of diplomats and politicians were intercepted and leaked publicly. At the time of writing this paper, many countries had still only proposed a draft code of conduct on information security for consideration by the UN Secretary-General (Baseley-Walker 2014).

## Some Suggestions

### *Implications for South Africa*

South Africa leads as number one target of cyber-attacks. Already there are institutions and legal framework enacted to combat cybercrimes and cybercriminals. The country is on its toes using the instruments it has to ensure its economy and all sectors relying on cyberspace to do business can feel secured. The challenge remain with effective public education because the majority of people rely on cellphone internet connections for all kinds of things today. There are proliferation of mobile apps which enable ordinary people to transact various activities and saving time. But the danger of apps being malware remain and it will take concerted effort starting at school level into the communities. Companies must be encouraged to translate some of their Corporate social responsibility activities into funding cyber security education of communities.

### *Implications for the Region*

**a) Security Policy and Assurance**

i. There ought to be effective collaboration of key regional institutions to review and update policies of monitoring and prosecution of cybercriminals.

ii. Citizens in the sub-region must come under regular education too on the auspicious danger of cybercrime in the use of indispensable IOT.

iii. Convergence of legal framework is essential to hasten dealing with cross-border cybercriminal activities.

iv. The mobile network and internet services providers to collaborate in regular campaign and education of the public using short messages (sms) in

understandable language can also go far to help protect users of mobile devices and computers from the crafty activities of cybercriminals.

v. Above all as proposed by Dawson, (2017) 'Developers of nongovernmental systems should start using policy, guidance, and directives to formulate baselines'.

**b) Early Detection and Response**

i. Effective monitoring comes with early detection of cybercriminal activities which remain highly unpredictable with their next criminal actions.

ii. Effective collaboration of states' security agencies and the partnership with private sectors cyber security agencies can be harness to hasten quick actions before deeper harms are caused by cyber-attackers.

**c) Security Training and Programs**

i. The need for regular training for all stakeholders in the sub-region is essential for ensuring the responsible institutions and agencies are all enriching the collaboration and partnership.

ii. Seminars and conferences are useful to attract wider coverage of people for raising public awareness through advertisements and publications of some of proceedings in local news dailies.

**d) Promotions and Publicity**

i. The use of the internet and digital facilities should be promoted in African communities as the inevitable paradigm. This can be done effectively using billboards and posters in communities in understandable local language. The faster people adjust to the digital environment also can help mobilise themselves to community education.

ii. The publicity aspect should focus on cautionary measures on dos and don'ts which in places like Zimbabwe some banks have bought FM radio slots to

educate their customers and the public daily on internet and mobile banking dangers and how to avoid them.

iii. The promotion and publicity of cyber security matters across the sub-region must be tired to some of the suggested activities above.

## Conclusion

In conclusion the paper reviewed the landscape of cybercrimes and cyber security of the global cyberspace in recent times. Indeed, the matter of cybercrimes and cyber security can fill volumes of pages even for a small region as southern Africa. Therefore, the discussion is just the tip of issues in the context of cyberspace and internet of things (IOT). The paper cast a brief glance on background of cybercrime and cyber security and looked at the situation of cybercrimes globally and on the African continent. The study found that Africa in particular is on the entry level pertaining to the use of the internet and much of what is happening is with mobile telephony areas which has allowed many ordinary people to explore the use of banking apps and involvement in social media activities. African institutions and companies have made in-roads especially the growing economies on the continent in West, East, Central and Southern Africa regions with lot of automation of bureaucracies, business transactions and banking, industries, outsourcing, online market, etc. It is a truism in the coming times Africa as a region could expand on its share of the cyberspace activities for as people and institutions and organisation digitize their transactional processes; besides the benefit in terms of financial value through activities on the internet would increase in Africa. However, in view of that the activities of cybercriminals have not been less on the continent either with the level of growth of internet activities and usage. The policy contention remain as to how much collaboration of all stakeholders on the continent in regard to government and businesses or the private sector. The study discovered some challenges which can be taken advantage of by cybercriminal and that is acting in isolation by countries in the African region. Even it clear that continental collaboration alone is not enough unless it is tied in tandem with the entire global community considering the amorphous nature of cybercriminals and the crimes they commit using different root locations to attack targets elsewhere. Much of the suggestions made regard making collaboration of the regional and global watchdogs effective as PPP matter; as nevertheless, the evil of cybercrime is here to stay but how to mitigate the effects and bring cybercrime proliferation

under control remain a day-to-day activity and actions of the collective global cyberspace monitoring stakeholders.

## References

Alharam, A.K. & W. El-madany 2017. *The Effects of Cyber-Security on Healthcare Industry.* 9th International IEEEGCC Conference, 08 – 11 May 2017. Manama, Bahrain. https://ieeexplore.ieee.org/xpl/conhome/8424857/proceeding https://doi.org/10.1109/IEEEGCC.2017.8448206

Australian Computer Society 2016. Cybersecurity: Threats, Challenges, Opportunities. Australian Computer Society November. https://www.acs.org.au/insightsandpublications/reports-publications/cybersecurity-threats-challenges-opportunities.html

Baseley-Walker, B. 2014. The UN Structure: The Intersection of Cyber Security and Outer Space Security. *International Security* December: 46 - 48. https://nsarchive.gwu.edu/sites/default/files/documents/5014652/United-Kingdom-Government-Chatham-House-Research.pdf Cf. also 2023 updated. https://finabel.org/wp-content/uploads/2023/07/May-2023.pdf

Baylon, C. 2014. Overview: Common Challenges in Cyber Security and Space Security – Contributing to an Escalatory Cycle of Militarization? *International Security* December: 7 - 15. https://nsarchive.gwu.edu/sites/default/files/documents/5014652/United-Kingdom-Government-Chatham-House-Research.pdf

Dawson, M. 2017. *Cyber Security Policies for Hyper Connectivity and Internet of Things: A Process for Managing Connectivity,* Missourri: s.n. https://www.academia.edu/34174191/Cyber_Security_Policies_for_Hyperconnectivity_and_Internet_of_Things_A_Process_for_Managing_Connectivity; https://doi.org/10.1007/978-3-319-54978-1_116

Dawson, M., M. Lieble & A. Adeboje nd. *Open Source Intelligence: Performing Data Mining and Link Analysis to Track Terrorist Activities*. https://link.springer.com/chapter/10.1007/978-3-319-54978-1_22;

Department of Jutice and Correctional Services – Republic of South Africa 2016. *Cybercrimes and Cybersecutiry Bill* s.l.: DOJS, Repubic of South Africa. Available at:

https://www.gov.za/sites/default/files/gcis_document/201703/b6-2017cybercrimes170221a.pdf

Dervojeda, K. *et al*. 2014. *Innovative Business Models for Competitiveness: Social Media for Internationalisation.* s.l.:s.n.

Gercke, M. 2012. *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* Geneva, Switzerland: International Telecommunications Union (ITU).

Hunter, S. 2016. *There's a Reason Cybercrime is So Bad in SA – And it's Kind of Scary.* Online not aviallable anymore.

Internet Life Stats 2016. *Internet Users by Country 2016.* https://www.internetlivestats.com/internet-users-by-country/

Jolly, C. 2014. *An OECD View: The Growing Risks of Satellite Signal Interference. International Security* December: 44 - 45.

MIT Center for Digital Business, n.d. The Digital Advantage: How Digital Leaders Outperform their Peers in Every Industry. https://ide.mit.edu/sites/default/files/The_Digital_Advantage__How_Digital_Leaders_Outperform_their_Peers_in_Every_Industry.pdf

Morgan, S. (Editor-in-Chief.). 2017. 2017 Cybercrime Report. Cybersecurity Ventures https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

O'Reilly, T. 2008. *Online Crackdown on Child Porn.* Available at: https://www.mediaclubsouthafrica.com/themedia/599-antichildpornsite04082008 (Accessed in 2018).

Pahi, T., M. Leitner & F. Skopik 2017. *Data Exploitation at Large: Your Way to Adequate Cyber Common Operating Pictures.* Vienna: ECCWS. https://www.researchgate.net/publication/323605024_Data_Exploitation_at_Large_Your_Way_to_Adequate_Cyber_Common_Operating_Pictures

Paryag, E. & A. Griffin nd. *What You Need to Know About Cybercrimes.* s.l.: s.n.

Reddy, G.N. & G.U. Reddy, n.d. *A Study of Cyber Security Challenges and its Emergning Trends on Latest Technologies.* https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies

Rojanasakul, M. & P. Coy 2017. *Companies that Use Robots Instead of Humans.* Available at: https://amp.businessinsider.com/companies-that-use-robots-instead-of-humans-2016-2

Serianu Ltd 2016. *Africa Cyber Security Report. 2016.* https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

Shiloh, J. & A. Fassassi 2016. *Cybercrime in Africa: Facts and Figures.* (Accessed in July 2018.) https://www.scidev.net/sub-saharan-africa/features/cybercrime-africa-facts-figures/

Singh, K. 2017. *Cybercrime Crooks Caught in SA Convicted by US Court.* https://www.news24.com/cybercrime-crooks-caught-in-sa-convicted-by-us-court-20170208

The Boston Consulting Group, Inc. 2012. *The Value of Our Identity.* s.l.: Liberty Global, Inc. https://www.libertyglobal.com/wp-content/uploads/2022/08/The-Value-of-Our-Digital-Identity.pdf

The SAGE Group 2017. *Cyber Security: Understanding the Cyber World. Law Enforcement Mentoring Solutions.* s.l.: s.n.

ThreatMetrix Digital Identity Network 2018. *2018 Cybercrime Report.* s.l.: ThreatMetrix. https://solutions.risk.lexisnexis.com/tmccr?t&source=linkedinwblog

Verma, A.K. & A.K. Sharma 2014. Cyber Security Issues and Recom-mendations. *International Journal of Advanced Research in Computer Science and Software Engineering* 44, April: 629 - 634. https://www.scribd.com/document/414438246/Cyber-Security-Issues-and-Recommendations

Yadav, S., T. Shree & Y Arora 2013. Cyber Crime and Security. *International Journal of Scientific & Engineering Research* 4, 8: 1 - 7.

Yassir, A. & S. Nayak 2012. Cybercrime: A Threat to Network Security. *International Journal of Computer Science and Network Security* 12,2, February. https://doi.org/10.1016/S1353-4858(12)70020-X

Yedaly, M. & W. Wright 2016. *GFCE Initiative: Cybercrime & Cybersecurity Trends in Africa.* https://securitydelta.nl/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf

Dr. Isaac Luthuli
University of KwaZulu-Natal
Department of Education
South Africa

# Chapter 6: Brazil, South - South International Security Governance and Peace Operations (2003 - 2016)[1]

**Kai Michael Kenkel**
**ORCID iD: https://orcid.org/0000-0003-4356-9304**

## Abstract

This paper explores Brazil's recent contributions to South – South governance and a rethinking of cooperation between global Southern states, as they relate to issues related to international security. Humanitarian intervention – the use of military force to protect individual rights and uphold the principles underpinning the international system – stands as proxy in this instance for the country's participation in collective security measures and the provision of peace and stability at the global level. Brazil's contribution to a notion of security governance anchored in the Global South will be assessed through a focus on both material aspects – participation in United Nations-led peace operations (and non-participation in Western-led initiatives) and ideational aspects such as debates on the norms governing intervention practice and those regulating the practice of security governance in multilateral bodies. Here, the country's engagement with the 'responsibility to protect' is one example.

**Keywords:** Brazil, peace operations, BRICS, responsibility to protect, Global South

This article explores Brazil's agency in South – South governance and within the BRICS, as they relate to issues related to international security, and highlights several ways in which Brazil has participated therein. It begins with an overview of Brazil's historical and current foreign policy positions with

[1] This manuscript was originally finalised and submitted for publication, in November 2018 and last revised in December 2020.

regard to global governance on the whole, covering both global-level organizations and the search for 'alternative geometries' emphasizing cooperation among states in the Global South. Global governance aspects are an important component of the country's quest for recognition as an emerging global player. Security issues – the focus of the subsequent section – have played a crucial part in this project, which was initiated by the Lula da Silva Workers' Party government in 2003 and has experienced a slowdown since the controversial impeachment of his successor in 2016.

Security issues have presented Southern emerging powers with a dilemma, in that changes in Western-led security practice have distanced traditional avenues of middle-power participation such as humanitarian intervention from postcolonial states' traditional normative commitments. Brazil's contribution to security governance will be assessed through the lens of Global South cooperation, through a focus on both material aspects – participation in United Nations-led peace operations (and non-participation in Western-led initiatives) – and ideational aspects such as debates on the norms governing intervention practice and those regulating the practice of security governance in multilateral bodies.

## Brazil and Global South Cooperation: Material & Ideational Aspects

### *Brazil and Global Security Governance*

Brazil's approach to security governance is influenced both by its overall engagement with global governance, and by historical specificities related to security, war and peace. Under the Workers' Party (PT) governments of Lula da Silva (2003 - 2010) and Dilma Rousseff (2011 - 2016), the country has expanded its foreign policy horizon on a global level, taking on a clear role as an emerging power, primarily through the BRICS grouping. Particularly the country's engagement with the institutional architecture of global governance – and its liberal normative content – have been portrayed in recent scholarship through use of the emerging power moniker. Definitions of what constitutes 'emergent' or 'rising' status abound in the literature, many focused on the interaction of these states with mechanisms of global governance. Here, the focus will be on two concurrent elements that bind these definitions together and relate specifically to Brazil's recent position on global governance: the existence of a clear hierarchy within the international system, and the concept of international responsibility in maintaining that hierarchy.

Taken together, these two elements lie at the root of oft-posed questions on the relationship of emerging powers such as the BRICS countries to the existing global order. Will these powers seek to ascend while still submitting to the extant conditions governing their rise, or will they seek, as they emerge, to reshape the rules of the system and of their own rise? In other words, are these powers revisionist or revolutionary (Lipton 2017)? Will they balance or bandwagon in relation to the established powers (Hurrell 2006)?

## *Hierarchy*

One distinction regarding hierarchy is of particular relevance to the BRICS and rising powers from the Global South. This is the divergence between essential acceptance of the normative content of what is fundamentally a liberal world order (Nel 2010: Mitzen 2011: 22), and their rejection of the formal and normative hierarchy behind it. This tension mirrors the distinction between the normative content of the liberal order in the economic realm – where emerging powers' preferred area of action lies (Kahler 2013: 714) and whose tenets they have challenged rhetorically (Laïdi 2012) if not consistently in content – and in the security arena, where postcolonial experiences have pushed normative preferences in a fundamentally different direction.

The rift between normative acceptance and the rejection of hierarchy runs through the contributions to Oliver Stuenkel and Matthew Taylor's recent volume *Brazil on the Global Stage* and is summarizes succinctly in their introduction (Stuenkel & Taylor 2015: 6 – 7). Both these authors and Merle Lipton (2017: 43) return to John Ikenberry's axiom that the Western-led liberal order is 'easy to join … and hard to overturn' (Ikenberry 2011: 56ff). Hierarchy is the fundamental characteristic uniting these two aspects. For emerging powers, this can result in the application of a double standard. Put succinctly, the international system is constructed in such a way that action in pursuance of national interests and preferences by established major powers is taken to be consistent and rational, whereas the same type of action, when performed by emerging countries such as the BRICS, is deemed 'ambiguous' (Stuenkel & Taylor 2015: 8), 'incoherent' (Lopes *et al.* 2013), 'irresponsible' (Patrick 2010) or 'reluctant' (Destradi 2017). In fact, however, emerging powers are increasingly recognized to be no less consistent and considered, or more exceptionalist, in their actions than their more powerful counterparts (Kahler 2013: 712,716: Lipton 2017: 6: Mares and Trinkunas 2016: 12: Burges 2013: 578).

## *Responsibility*

In the context of global governance, particularly of security issues, this hierarchy manifests in how one of the key subjacent concepts of that order – responsibility – is defined and attributed. Both the normative content of collective security and the acceptable manner of its implementation remain the province of established powers. Similarly to the liberal order itself, as the R2P debate shows, this has generated broad agreement on normative content and extensive contestation of how the concept is to be implemented. While few dispute that with increased power comes increased pressure to contribute actively to solving crises – strong divergence remains over how this is to be achieved.

Amrita Narlikar has given this correlation familiar theoretical terms by equating responsibility with the provision of a global public good (Narlikar 2011: 1608). While great power expectations have centered on dividing the labor of implementing global governance, emerging powers have asserted their claim to participation in defining the nature of the inherent responsibility, while to taking pains not to be seen as 'free riders' particularly in the security sphere (Abdenur 2017: 86: Culp 2016: 1529).

As noted with respect to the liberal order itself, one primary dilemma for postcolonial rising powers is the divergence between how the North sees fit to implement, for example, collective security decisions – through the use of force – and their historically grounded aversion to doing so in this manner. These powers' relative weakness in terms of hard military power, coupled with political preferences that privilege other areas of policy – has placed them at a disadvantage where hierarchy equates Northern preferences with global collective preferences (Kenkel & Martins 2016: Bukovansky *et al.* 2012: 27 – 32). Indeed, this perceived conflation of Northern with global collective interests has been a driving force of emerging powers' quest for alternative geometries of global governance (Hurrell 2010a: 62: Hirst 2015: 364) highlighting the Global South, or what Narlikar terms 'club goods' (Narlikar 2011: 1609).

## *Norm Diffusion*

The privileging of security issues and military force has dislocated emerging powers' challenge to soft power issues and to the normative arena (Mares & Trinkunas 2016: 14 - 15: 86 - 88), where effective contestation of the definition of key rules and concepts can take place. Several analysts have noted the

corollary that emerging powers are effectively precluded from taking a direct approach to pursuing their own interests, 'aware that efforts to forcefully impose [their] power would actually undermine [their] position both regionally and globally' (Hoffmann *et al.* 2016: 843: Flemes & Vaz 2011). Asserting themselves in this complex environment in a manner reflective of their newfound status has placed emerging powers before what some analysts have termed a 'graduation dilemma' (Milani *et el.* 2017) which highlights the increasing complexity both of the international environment, and of these states' internal political frameworks as they consolidate internally and take on a larger international presence (Kenkel & Harig 2017).

Greater complexity in the normative practice of global governance has been accompanied by increased sophistication in the academic analysis of how norms and ideas diffuse, and participation in their definition managed. Norms scholarship is fundamental to understanding Brazil's vision of its contribution to global governance. Norms theory in constructivist International Relations is often described as having moved through at least three 'waves'. The first, embodied by the 'life cycle' model developed by Martha Finnemore and Kathryn Sikkink (1998), was a decisive challenge to material and state-based accounts of behavior, but did not move beyond a unidirectional conception allowing merely for either acceptance or rejection by 'receiving' states (Finnemore & Sikkink 1998; Risse, Ropp & Sikkink 2013). The second 'wave' focused on internal processes of institutionalization in those receiving states (Cortell & Davis 2000; Checkel 1997). The third focused on normative content itself and allowed for diffusion to be viewed as a bidirectional process (Acharya 2009: Solingen 2012: Pu 2012. Only with this third wave was it possible to address the agency of emerging powers in the process, beyond simple recipients of content of Northern origin (Acharya 2014; Mitzen 2011: 57). Recently norm diffusion has come to be understood not only as a multidirectional, but as a non-linear and complex, process (Hunt 2016), and studies have moved beyond formal institutionalization to focus on the meaning attributed to a norm once it is placed in practice (Wiener 2009) or implementation (Betts & Orchard 2014).

Antje Wiener's approach is eminently relevant to emerging powers' role in the diffusion of global norms. It claims that formal institutionalization is less crucial to the validity of a norm than its legitimacy as viewed by its users during the process of its definition and contestation. This legitimacy is derived from the regular access of all stakeholders to the contestation process (Wiener 2014: 3). Where structural approaches equate validity with an uncontested fixedness of content, Wiener concludes the inverse (Wiener 2014: 22). The

radical inclusiveness of this approach is especially attractive to emerging powers, and is a crucial component – not grasped by the main currents of scholarship in the Global North – of explaining their conduct, particularly in the security sphere where they often lack hard power.

## Brazil and Security Governance

International security is perhaps the area where the factors outlined above come most clearly to the fore: it is both the area of international diplomacy where formal decision-making is at its most hierarchical and exclusive, and that where (ultimately Western-based) notions of responsibility as a prerequisite for participation are most entrenched. This is not to imply that other areas of policy have not arisen where emerging powers have been involved in discussions of responsibility and load – sharing; prominent other topics include free trade (Hopewell 2014); climate change mitigation (Hochstetler & Milkoreit 2015); and nuclear disarmament and non-proliferation (Narlikar 2011: 1608). Nevertheless, the security agenda continues to occupy a privileged position in international decision-making.

This section will present how Brazilian policymakers have positioned the country in this area of policy and highlight several areas where the country has been particularly active in maintaining a security policy presence, and where a concerted effort has been made to act in concert with the BRICS and the Global South. Finally, this section will investigate whether the Brazil's preferred alternative to global multilateral bodies, the BRICS grouping, has been able to consolidate into an effective actor on issues of collective security.

### *Brazilian Normative Priors on Security*

Brazil's approach to international security governance is a mixture of South American security culture, classic emerging power behaviour, and the legacy of colonial history. From regional security culture Brazil takes first and foremost two elements: a penchant for multilateralism and a strict adherence to the principle of non-intervention. Multilateralism is seen above all as a double guarantee. On the one hand, a rules-based order rooted in the normativization and legalization of international relations limits the effects of disparities in hard power capacities, protecting against potential interference from major powers (Adebajo 2016: 1188). On the other, multilateral forums provide an ambit in which these inequalities are further reduced by the principle of equal

representation. Emerging powers tend to share this similarly predilection for multilateralism, as it provides them a stage upon which to potentially 'punch above their weight' and attain greater policy effects relative to their investment of diplomatic or material capital (Kenkel 2010; 2013c).

South American states share the second with other postcolonial states: a strict adherence to the principle of non-intervention. Whereas in South America this is coupled with commitment to the pacific resolution of disputes, this is not true of all areas of the Global South. What remains as a commonality is the *de facto* equation of the principle of state sovereignty with non-intervention, non-interference and the inviolability of borders.

Many consider this externally-oriented interpretation of sovereignty to have contributed to 150 years of interstate peace in the region. Changes in the West, driven by genocides and mass atrocities such as those in Rwanda, Kosovo, Somalia and Bosnia, have not generated the same shift to an internal, contractual notion of sovereignty inclusive of the protection of individual rights (Kenkel 2012). In South America, emphasis on human rights and democratic governance tends to be external and collective (emanating from the state itself), rather than internal and couched in terms of individual rights.

Further elements of regional security culture include a penchant for legal normativism and a clear aversion to the use of military force as a means of conflict resolution. Indeed, most regional military establishments are not equipped to project force at a sustained meaningful level. Arie Kacowicz lists the further common tenets of the purported South American 'region of peace' [2] as the recognition of colonial borders, including through *uti possidetis*, popular self-determination; convivencia (peaceful coexistence); concertación (decision by consensus); confidence-building measures, especially regarding disarmament and nonproliferation; and democracy and human rights (Kacowicz 2005).

Recent Western-led changes within global multilateral institutions, as well as emerging powers' – and Brazil's – relative ascension in the international hierarchy, have cast into doubt a number of these precepts. Alongside non-intervention and the non-use of force, the main notion affected here is the legitimacy of the United Nations Security Council – once a fixed element at the

[2] One effect of this notion of sovereignty is that is has created a disjunction between external peace and internal violence: while the region has seen no major conflict in 160 years, it cannot in good faith be referred to as a 'zone of peace': violence rates are among the highest in the world – Brazil alone loses over 60,000 citizens a year to gun violence alone.

core of Brazilian foreign policy (Cervo 2010: 11) as a decision-making body without Southern representation (Binder & Heupel 2015). Andrew Hurrell has, however, described these efforts as still 'very much within the system' (Hurrell 2010b: 136).

One further Brazilian strategy of note, highlighted by Monica Hirst (2015: 362 - 363) has been to seek to integrate development and security issues. Given Brazil's success, under the PT governments, with both internal development and foreign technical cooperation (largely on a South - South basis) (Dauvergne & Farias 2012), coupled with its aversion to (and lack of sustained capacity to project) military force, there is strong incentive to unite these two issues. Peacebuilding, as will be shown below, provides the opportunity to make a virtue of necessity by attaining a security impact by doing development.

## *Brazil in its Region*

The literature on Brazil's interaction with its region is understandably vast, and the purpose of this section is to highlight selected aspects of it that relate to the country's participation in security governance from a South - South perspective. Two aspects are most relevant here. *First*, changes in the norms underpinning security governance at the global level – mainly the shift towards protection of individual rights, driven by the genocides of the 1990s – have created a tension between a regional security culture largely unaffected by these shifts, and a divergent set of expectations governing the responsibility of putative global-level players (Kenkel 2012: Kenkel & De Rosa 2015: Kenkel & Stefan 2016). This tension is at the core of the analyses of peace operations and R2P that follow. *Second*, Brazil's aspirations to global player status do not have the regional support necessary to translate cleanly into a representative role at the global level (Kahler 2013: 724). The result is a disconnect between Brazil's approach to it regions and its regional aspirations. Additionally, since 2016 Brazil and the region itself have experienced political polarization and realignment.

Andrés Malamud points out that regional leadership has not been the springboard to a global role to which Brazilian policymakers had aspired, due both to clashing aspirations in the region and difficulties and shortcomings in institution-building (2011). As the country's policy horizon has shifted to the world, regional policy has turned towards a coalition-building function between the West and the Global South (Burges 2013). Whereas some authors have been quite critical of Brazil's selective investment in firming up institutions in its

immediate environs (Burges & Daudelin 2007), others have placed it within a framework of a resource allocation dilemma for emerging powers. Hofmann *et al* 2016) point out that ideological disparity within a region raises the incentive to invest diplomatic resources at the global level (2016) and to 'forum shop' regionally. Paradoxically Brazil's ability to exercise regional leadership is also hampered by its very preponderance in the region. As a result, the country has pursued a strategy of leadership which effectively replaces coercion with soft power, which Sean Burges has termed 'consensual hegemony' (2008). Consensual hegemony also involves the discursive projection of new common geopolitical spaces in which actors such as Brazil can exercise a leadership function. Recently, one such space for Brazil has been the South Atlantic, in part as a gateway to greater economic and geostrategic presence on the African continent.

## *Brazil, the South Atlantic and Africa*

The past decade has seen renewed Brazilian interest in the South Atlantic region. Though it is largely spurred by the discovery of extensive oil reserves in the pre-salt regions on the continental shelf, this focus possesses important synergies with the country's emerging power project, especially as it relates to potential connections to Africa. Under the guise of the 'Blue Amazon' – a term alluding to the economic and strategic importance of the country's vast rain forest – Brazil has been engaged in the discursive creation of a regional security complex, or at least a shared security consciousness, in the South Atlantic region (Mattos *et al.* 2017; Abdenur & Marcondes 2014a; 2014b). This has led to a recrudescence of efforts to systematize the country's overall approach to maritime security (Duarte & Barros forthcoming). This initiative serves both to protect Brazilian economic interests in the region, and to exclude 'extraterritorial powers' – read great powers – from the region. Efforts have been made to revive the Zone of Peace and Cooperation in the South Atlantic (ZOPACAS), and several studies have highlighted the importance of this region to both the BRICS and IBSA (Abdenur *et al.* 2014: Vaz 2015).

The African continent was a declared foreign policy priority of the Lula da Silva government (2003 - 2011). So many new embassies were opened on the continent that Brazil's representation there surpassed that of major powers such as the USA, France and the UK (Kenkel 2013b: 274). The vast majority of interaction between Brazil and Africa has been focused on South - South technical cooperation and aid, within an optic of exporting the successes of Brazil's

own domestic fight against underdevelopment and particularly inequality (Kenkel 2013b: Abdenur 2015: 215: Mello e Souza 2015: Stolte 2015).

However, Brazilian cooperation on defense and security matters with African partners has remained within discreet proportions, and has occurred as a result of direct contact between military establishments, such as in the cases of Namibia (Seabra 2016), São Tomé and Gambia. The exception is Guinea-Bissau, where the country has invested extensively in both bilateral and multilateral peacebuilding initiatives (Abdenur & Marcondes 2014c; Neves 2010). Peacebuilding – and the development of a putative Brazilian approach – is a major part of the country's drive to demonstrate its capacity to contribute to collective security measures through global-level multilateral mechanisms. While the United Nations remains the country's chosen avenue for action on security – though not other – governance measures, it has sought to act through the BRICS mechanism as well, though in this arena the grouping has had at best mixed success.

## *BRICS and Security*

Whereas the BRICS arrangement has made significant strides in offering alternatives to the liberal, Western-led global economic order – as in the case of the New Development Bank – divergences in both regime type and foreign policy preferences – including established power status – have hampered its ability to produce results as a contributor to collective security. In the naval arena, the IBSA group, without the presence of the two UNSC permanent members, has held joint maritime exercises and sought to provide comparative insights between the South Atlantic and Indian Ocean contexts (Vaz 2015).

As an emerging power grouping, the BRICS have sought to provide alternatives to conflict resolution beyond the UN Security Council, though these have repeatedly been dashed on the rocks of Russian and Chinese intransigence with regard to the major conflicts of the day. The two UNSC permanent members have effectively controlled the BRICS security agenda, a domination which became very clear during the group's attempts to address the Crimean and Syrian conflicts. As a loose transregional coalition of states with highly divergent security interests, the BRICS' ability to engage in agenda-setting and to identify areas of effective cooperation in alternative approaches to conflict resolution has been quite limited (Abdenur 2017: 79 - 84). Discursively, one of the group's main contributions has been to cement claims that the global

security context is now clearly multipolar, involving the necessity to accommodate the growing weight of the Global South[3].

In terms of concrete practice, however, particularly as regards efforts to employ hard power jointly, in the security realm the BRICS have failed to provide a serious alternative for countries like Brazil to work outside the global liberal institutions: the Syrian war provides a striking example. The BRICS' position on the Syrian conflict has from its inception been heavily influence by the aftermath of the NATO intervention in Libya (see the section on R2P below), during which all five members occupied seats on the UNSC and were nonetheless unable effectively to influence the outcome of the conflict. Their skepticism translated into hesitance to condemn the gross human violations of the Assad government despite, for example, Brazil's long-term rhetorical commitment to human rights protection (Abdenur 2016a). As the conflict progressed and Russia's proactive role in supporting the Assad regime became incontrovertible, Moscow dominated the group's agenda-setting with regard to the conflict, leading to its reframing as a matter predominantly of terrorism (Abdenur 2016a). A similar dynamic shaped the group's one-sided response to the invasion of Crimea by Russia. In this sense, following the logic laid out by Hofmann *et al.* 2016) for regional contexts, divergences between the members have meant that global-level forums have remained – in the security realm – the more effective alternative for Brazil to contribute to global governance. It has done so over the course of the past 15 years by means of significant participation in peace operations and in the normative conversation regarding intervention in the name of atrocity prevention (R2P).

## Brazil and Peace Operations

Brazil has participated in collective security measures since its tenure in the League of Nations. With regard to UN peace operations, the country was, until 2004, with a few notable exceptions, a provider mostly of 'token' (Coleman 2013), mostly individual, contributions (Fontoura 2009; Cardoso 1998; Aguilar 2005; Uziel 2016). From 1957 to 1999, Brazil contributed over 11 000 troops, and more than 300 policemen, the vast majority of which served within the UN Emergency Force (1956 - 1967) in Suez. The further notable contributions were

[3] Amitav Acharya has dubbed this a 'multiplex world' (2017), whereas resistance to a de facto departure from unipolarity has come from Ikenberry (2008) and colonial apologist Bruce Gilley (2016.

an 800-man battalion to the UN Angola Verification Mission III (UNAVEM 1995 - 1997): civilian police in East Timor (UNTAET – 1999-2002) and a smaller force to Mozambique (UNOMOZ 1993 - 1994). This sparse presence in peace operations was due both to military operational limitations and to the translation of the country's foreign policy traditions into a strict distinction between participation in Chapter VI missions, and avoidance of Chapter VII missions, which involve authorization of the robust use of force (Kenkel 2012).

Profound change occurred in 2004 with the creation of UN Stabilization Mission in Haiti (MINUSTAH). The Global South emerging power project pursued by the Lula government identified in this mission the opportunity to present Brazil as a responsible power and as a provider of collective goods in the security arena (Kenkel 2013c: 96). One of the explicit goals of this project was to reform the hierarchy of global governance in Brazil's favor – including through diplomatic cooperation with the BRICS – and eventually to enshrine the country as a permanent member of the UNSC. Until its closing in 2017, Brazil provided MINUSTAH's largest contingent, its military commander, and led policy coordination efforts between the Latin American states who made up more than half of its troops (Kenkel 2010: 2013c).

In quantitative terms,

> Prior to the January 2010 earthquake, Brazil had deployed approximately 1,300 troops, whose area of responsibility in the capital of Port-au-Prince encompassed approximately 1.5 million people, about one-sixth of Haiti's population. These troops consisted of a full Army battalion, a Marine Corps battle group and an Army engineering company. Immediately following the earthquake this was increased by a second Army battalion of about 900, tasked exclusively with humanitarian relief. … In acquitting themselves successfully of tasks typical of peace enforcement, in tactical terms Brazilian troops acted little differently from other contingents involved in other robust Chapter VII missions (Kenkel 2013c: 101.

MINUSTAH provided proof that the aspiring South American power was willing to go beyond discourse in its contribution to international security: its total expenditure over the mission's period of deployment reached 2.5 billion reais (1 billion USD): expenditures on direct participation in MINUSTAH were only partially reimbursed (Stochero 2017). The nature of this expenditure is significant in that a proportion of it took place outside of MINUSTAH proper.

Brazil initiated, within the Haitian context, a concerted effort to create its own paradigm of development aid and technical assistance. Designed to constitute an alternative to the Northern-led liberal peace paradigm (Richmond 2006), this approach was based on the idea of exporting the successes experienced by PT-led social programs at the domestic level.

The Brazilian peacebuilding approach is innovative in that it combines elements from across the range of government programs, from classic security and development actors to agricultural innovation, basic health services and conflict resolution NGOs. It is based on accompanying efficient military contingents with support for local ownership: political emphasis on institution-building, and economic focus on sustainability: and on close contact with population and on historical, cultural affinities. This latter characteristic has been shown to limit the exportability of the approach in the African context (Kenkel 2013b; Abdenur & Call 2017). Additionally, the approach was hampered by the same difficulties that permeate the Brazilian domestic context: financial constraints, myopic policy planning, and inconsistent delivery. Nevertheless, there is significant innovation in the approach's content, which alongside its utility as a key component of an emerging-power strategy has generated a strong sense of exceptionalism about the country's role as a source of alternatives to the liberal peace (Hirst 2015: 368). This has given rise to a certain gap between the discourse and the reality of the country's role in peacebuilding, although Brazil has been instrumental in bringing to the fore the connection between security and development in successful peacebuilding (Kenkel 2013b; Abdenur & Call 2017: 31: 22).

Brazil's strict adherence to the limitations of Chapter VI of the UN Charter as authorization for missions' mandates limits the utility of UN peace operations as a conduit for influence. The vast majority of missions are now authorized under Chapter VII and are involved in robust missions for the protection of civilians. This stands in direct contrast to Brazil's preferred approach to assistance under the guise of BRICS-based South - South technical cooperation. This normative tension is at the core of the country's successful involvement in the ongoing evolution of humanitarian intervention norms at the UN and elsewhere. Indeed, Brazil's acquiescence to participating prominently in a Chapter VII mission, and later expanding its contribution to other contexts – the country has a major maritime contingent in UNIFIL in Lebanon – has both shored up its position as an important contributor to global security governance and generated growing critique of this 'subaltern' role from sceptics with a postcolonial viewpoint within the country (Moreno *et al.* 2012: Blanco 2017).

## Brazil and Intervention Norms: R2P and RwP

The Responsibility to Protect (R2P) is a political norm designed to reconcile state sovereignty with the protection of civilians against mass atrocities and genocide (Bellamy 2011: Thakur 2011). Developed by an international commission convened by Canada in 2000 (ICISS 2001), the purpose of its creation was, *inter alia*, to create firm guidelines for UN Security Council decisions involving the use of force. Though its primary focus was not initially on military force, this aspect has generated almost all of the diplomatic and analytical debate on R2P. The concept has since been extensively institutionalized at the UN and elsewhere (United Nations 2005: paras 138 - 139: 2009). Very broadly writ, the initial reactions to R2P and its inherent potential for justifying the use of military force were positive in NATO member states and negative – despite buy-in to the overall notion of the event-driven necessity to prevent genocide – in the Global South.

As R2P came increasingly to shape the normative underpinnings of UN and NATO intervention practice, emerging powers who had elected these institutions as the channels of their contribution to global security (Job 2016) were faced with a growing gap between their own policy priors and UN practice (Kenkel & De Rosa 2015; Kenkel & Stefan 2016; Garwood-Gowers 2013; Stuenkel 2016). A crucial moment arrived with the NATO intervention in Libya in 2011. Its supporting Resolution, the UN Security Council explicitly grounded the intervention in R2P: however, the text was passed under circumstances that led to significant resentment from emerging powers. All five BRICS were members of the Council at the time: they were not involved in Resolution 1973's drafting and later claimed they had been misled as to the ultimate aims and means of the action mandated (Job 2016; Bloomfield 2015; Singh 2016; Garwood-Gowers 2013; Hunt 2016; Ralph & Gifkins 2017). Consequently, many emerging contributors to the global security commons turned even further away from R2P, and a conceptual rift ensued between its content – upon which almost all states of the world agree – and the preferred means of its implementation.

Brazilian diplomats, under the leadership of Foreign Minister Antonio Patriota, seized this opportunity for the country's first serious foray as a norm entrepreneur. Six months after the vote on Resolution 1973, Brazil circulated the concept of the 'responsibility while protecting' at the UN: it was designed to bridge the conceptual differences between Western and Southern powers on R2P, primarily through strict controls on Council practice and further limita-

tions on the use of military force. The concept's authors took as their point of departure the notion that 'one casualty is too many' as a result of interveners' actions (Gaskarth 2017: 304). This was roundly rejected by Western powers, who had internalized the counterfactual argument that many more lives might be saved through the loss of a few. Additionally, Brazil was not seen in the West as possessing the means to mount effective alternatives in favor of atrocity prevention if R2P were to be limited in this way, leading to accusations of a 'do as I say, not as I do' posture (Kelly 2013).

However, it soon became evident that the P-3's precipitated use of R2P to justify the Libya intervention had done serious damage to the concept's overall acceptance. This was particularly true in the case of Syria: in the words of ICISS member Ramesh Thakur, 'Syrians have paid the price of NATO excesses in Libya' (Thakur 2013: 70). The Syrian stalemate has been particularly trying for powers seeking to articulate alternatives to the Security Council, as the Russian government has assisted its Syrian allies in not only blocking action there but in the BRICS arrangement as well.

Despite the tarnished image of the R2P norm itself in the face of crimes in Syria and other ongoing conflicts, the debate over the concept has become an important locus for emerging powers to exercise soft power, to participate in the normative shaping of the key rules of the international order, and to participate in the provision of collective security goods at the discursive, behavior-structuring level. This participation has in particular been taken as a fruitful stage for the study of norm contestation (Wiener 2009: 2014) and, in particular the notion that in an increasingly multipolar order, norms no longer flow unidirectionally from one preordained set of states to another (Pu 2012; Stefan 2016; Shesterinina 2016; Acharya 2016). In this manner, Brazil's ongoing participation in these fora constitutes a key element in its quest to project, through both hard and soft power means, its intention to act as a provider of global goods in the security realm, and to partake of the greater level of participation in collective decisions that accrues to powers viewed as having proven their international responsibility through this channel.

## Future Prospects

Unfortunately for BRICS cooperation in the peacekeeping ambit, political changes in Brazil have totally revamped the country's attitudes to security governance over the past two years. The election of extreme right-wing candidate Jair Bolsonaro to the Brazilian Presidency from January 2019 has

brought a complete wind change to the country's foreign policy and ultimately international stature. Bolsonaro has abandoned traditional foreign policy principles and diplomatic praxis, and aligned the country with extreme-right wing leaders around the world. His foreign minister, Ernesto Araujo, has repeatedly endorsed conspiracy theories directed against multilateral institutions and both liberal and progressive values, as well as even coronavirus containment policies. Brazil's foreign policy was – until the electoral ouster of Donald Trump in November 2020 – aligned with Trump's personal political agenda and with Washington's interests, often to the detriment of Brazil's own societal needs.

The BRICS configuration and relations with the Global South have been relegated to ancillary status. Indeed the new leader's Vice President described African countries during the campaign as *mulambada*—a term originally applied to slaves of Angolan origin, which refers to poor, uneducated Blacks.[4] The result has been a precipitous decline in Brazil's global diplomatic stature at the UN: coupled with the government's unwillingness to confront, or even denounce, raging wildfires in the Amazon in 2019 and 2020, the country is on the cusp of international pariahdom.

Beyond the sidelining of relations with the Global South, two factors have further driven a withdrawal of Brazil from prominent or even relevant status as a peacekeeping troop contributor. First, as Brazilian foreign policy realigned, the abovementioned project for global influence and decisionmaking power – associated with the Workers' Party governments Bolsonaro won election by demonizing – was comprehensively abandoned. Cooperation with the African continent, and the BRICS as a whole (as a result of an ideologically-driven combative stance towards Beijing in particular), was decimated: it remains to be seen whether extensive military influence in the new government will allow peace operations to retain pride of place. However, the association of this project with the PT government, and its oftentimes anti-Western leanings, have reduced Brazil's search for protagonism through these avenues and placed them on an entirely different normative footing. Second, the move within UN peace operations from liberal peacebuilding – with local populations' well-being at its centre – to counterinsurgency-and counterterrorism-based stabilization missions both runs against Brazil's capacities and propensities as a troop contributor, and presents a significant risk to the quality of its now-threatened civilian control over the armed forces.

[4] https://www.significados.com.br/mulambo

Due to its current ideologically oriented foreign policy, Brazil has suffered a significant blow to its global relevance and the soft power bonus it enjoyed before the impeachment of Rousseff in 2016. Coupled with the economic hardships that began even before the coronavirus pandemic, it is likely to take Brazil a significant time to recover its role as a prominent peacekeeper and security interlocutor in the Global South. When it does do so, it is likely to be only once the current derailment of the country's traditional role, values and identity has been rectified by the return of non-extremist politics to power.

**Acknowledgement:** Research leading to this publication has received funding through research grants from the Brazilian National Council for Scientific and Technological Development – CNPq (Bolsa de Produtividade Nível 2) and the Rio de Janeiro State Research Foundation – FAPERJ (Cientista do Nosso Estado. It was further financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001.

## References

Abdenur, A. 2015. Organisation and Politics in South - South Cooperation: Brazil's Technical Cooperation in Africa. *Global Society* 29: 1 - 18. https://doi.org/10.1080/13600826.2015.1033384

Abdenur, A. 2016a. Rising Powers and International Security: The BRICS and the Syrian Conflict. *Rising Powers Quarterly* 1,1: 109 - 133.

Abdenur, A. 2016b. Rising Powers in Stormy Seas: Brazil and the UNIFIL Maritime Task Force. *International Peacekeeping* 23,3: 389 - 415. https://doi.org/10.1080/13533312.2016.1155413

Abdenur, A. 2017. Can the BRICS Cooperate in International Security? *International Organisations Research Journal* 12,3: 73 - 93. https://doi.org/10.17323/1996-7845-2017-03-73

Abdenur, A. & C. Call 2017. A 'Brazilian Way'? Brazil's Approach to Peacebuilding. In Call, C.T. & C. de Coning (eds.): *Rising Powers and Peacebuilding: Breaking the Mold?* Houndsmills: Palgrave MacMillan. https://doi.org/10.1007/978-3-319-60621-7_2

Abdenur, A., M. Folly, K. Moura, S.A.S. Jordão & P. Maia 2014. The BRICS and the South Atlantic: Emerging Arena for South - South Cooperation. *South African Journal of International Affairs* 21,3: 1-16.

https://doi.org/10.1080/10220461.2014.972442
Abdenur, A. & D.M. de Souza Neto 2014a. O Brasil e a cooperação em defesa: a construção de uma identidade regional no Atlântico Sul. *Revista Brasileira de Política Internacional* 57: 5-21. https://doi.org/10.1590/0034-7329201400101
Abdenur, A. & D.M. de Souza Neto 2014b. Region-Building by Rising Powers: The South Atlantic and Indian Ocean Rims Compared. *Journal of the Indian Ocean Region* 9: 1-17. https://doi.org/10.1080/19480881.2014.896103
Abdenur, A. & D.M. de Souza Neto 2014c. Rising Powers and the Security-Development Nexus: Brazil's Engagement with Guinea-Bissau. *Journal of Peacebuilding and Development* 9,2: 1016. https://doi.org/10.1080/15423166.2014.950118
Acharya, A. 2009. *Whose Ideas Matter? Agency and Power in Asian Regionalism*. Ithaca: Cornell University Press. https://doi.org/10.7591/9780801459757
Acharya, A. 2011. Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-Making in the Third World. *International Studies Quarterly* 55: 95-123. https://doi.org/10.1111/j.1468-2478.2010.00637.x
Acharya, A. 2014. The R2P and Norm Diffusion: Towards a Framework of Norm Circulation. *Global Responsibility to Protect* 5:4: 466-479. https://doi.org/10.1163/1875984X-00504006
Acharya, A. 2016. 'Idea-shift': How Ideas from the Rest are Reshaping Global Order. *Third World Quarterly* 37,7: 1156-1170. https://doi.org/10.1080/01436597.2016.1154433
Acharya, A. 2017. After Liberal Hegemony: The Advent of a Multiplex World Order. *Ethics & International Affairs* 31,3: 271-285. https://doi.org/10.1017/S089267941700020X
Adebajo, A. 2016. The Revolt against the West: Intervention and Sovereignty. *Third World Quarterly* 37,7: 1187-1202. https://doi.org/10.1080/01436597.2016.1154434
Aguilar, S.L.C. 2005. *Brasil em missões de paz.* São Paulo: Usina do Livro.
Bellamy, A. 2011. *Global Politics and the Responsibility to Protect: From Words to Deeds*. London: Routledge. https://doi.org/10.4324/9780203837160
Betts, A. & P.A. Orchard (eds.). 2014. *Implementation and World Politics: How International Norms Change Practice*. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198712787.001.0001

Binder, M. & M. Heupel 2015. The Legitimacy of the UN Security Council: Evidence from Recent General Assembly Debates. *International Studies Quarterly* 59: 238-250. https://doi.org/10.1111/isqu.12134

Blanco, R. 2017. The Brazilian Engagement with Peace Operations: A Critical Analysis. *Revista Brasileira de Política Internacional* 60:2: n.p. https://doi.org/10.1590/0034-7329201700206

Bloomfield, A. 2015. India and the Libyan Crisis: Flirting with the Responsibility to Protect, Retreating to the Sovereignty Norm. *Contemporary Security Policy* 36,1: 27-55. https://doi.org/10.1080/13523260.2015.1012347

Brazil – Permanent Mission of the Federative Republic of Brazil to the United Nations 2011. Responsibility while Protecting: Elements for the Development and Promotion of a Concept. 09 November. United Nations Document A/66/551-S/2011/701.

Bukovansky, M., I. Clark, R. Eckersley, R. Price, C. Reus-Smit & N.J. Wheeler 2012. *Special Responsibilities: Global Problems and American Power*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781139108812

Burges, S. 2008. Consensual Hegemony: Theorizing Brazilian Foreign Policy after the Cold War. *International Relations* 22,1: 65 - 84. https://doi.org/10.1177/0047117807087243

Burges, S.W. 2013. Brazil as a Bridge between Old and New Powers? *International Affairs* 89:3: 577-594. https://doi.org/10.1111/1468-2346.12034

Burges, S. & J. Daudelin 2007. Brazil: How Realists Defend Democracy. In Legler, T., S.F. Lean & D.S. Boniface (eds.): *Promoting Democracy in the Americas*. Baltimore: Johns Hopkins University Press.

Campos, P.R. & T. da Fontoura, 2009. *Brasil: 60 anos de operações de paz*. Rio de Janeiro: Diretoria do Patrimônio Histórico e Documentação da Marinha.

Cardoso, A.J.S. 1998. *O Brasil nas Operações de Paz das Nações Unidas*. Brasília: FUNAG.

Carmody, P. 2013. *The Rise of the BRICS in Africa: The Geopolitics of South - South Relations.* London: Zed Books. https://doi.org/10.5040/9781350223509

Cervo, A.L. 2010. Brazil's Rise on the International Scene: Brazil and the World. *Revista Brasileira de Política Internacional* 53, Special Edition: 7-32. https://doi.org/10.1590/S0034-73292010000300002

Checkel, J.T. 1997. International Norms and Domestic Politics: Bridging the Rationalist-Constructivist Divide. *European Journal of International Relations* 3:4: 473 - 495. https://doi.org/10.1177/1354066197003004003

Coleman, K. 2013. Building International Legitimacy: The Significance of Token Forces in Contemporary Military Interventions. In Bellamy, A. & P. Williams (eds.): *Providing Peacekeepers: The Politics, Challenges, and Future of United Nations Peacekeeping Contributions*. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199672820.003.0003

Cortell, A.P. & J.D. Davis, Jr. 2000. Understanding the Domestic Impact of International Norms: A Research Agenda. *International Studies Review* 2,1: 65 - 87. https://doi.org/10.1111/1521-9488.00184

Culp, J. 2016. How Irresponsible are Rising Powers? *Third World Quarterly* 37,9: 1525-1536. https://doi.org/10.1080/01436597.2016.1166046

Dauvergne, P. & D.B.L. Farias 2012. The Rise of Brazil as a Global Development Power. *Third World Quarterly* 33,5: 903 - 917. https://doi.org/10.1080/01436597.2012.674704

Destradi, S. 2017. Reluctance in International Politics: A Conceptualization. *European Journal of International Relations* 23,2: 315 - 340. https://doi.org/10.1177/1354066116653665 PMid:30166933 PMCid:PMC6097117

Duarte, É. & M.C. de Barros (eds.) Forthcoming. *The Global South in the South Atlantic: Regional Dynamics, Geopolitics and Maritime Security*. London: Routledge.

Finnemore, M. & K. Sikkink 1998. International Norm Dynamics and Political Change. *International Organization* 52,4: 887 - 917. https://doi.org/10.1162/002081898550789

Flemes, D. & A.C. Vaz 2011. Security Policies of India, Brazil and South Africa – Regional Security Contexts as Constraints for a Common Agenda. *GIGA Working Paper* 160. Hamburg: German Institute for Global and Area Studies. https://doi.org/10.2139/ssrn.1780208

Garwood-Gowers, A. 2013. The BRICS and the Responsibility to Protect: Lessons from the Libyan and Syrian Crises. In Sancin, V. & M.K. Dine (eds.): *Responsibility to Protect in Theory and Practice*. Ljubljana: GV Zalozba.

Gaskarth, J. 2017. Rising Powers, Responsibility, and International Society. *Ethics & International Affairs* 31,3: 287 - 311.

https://doi.org/10.1017/S0892679417000211
Gilley, B. 2016. Delusions of Grandeur in the Goldilocks Zone. *International Journal* 71:4: 651-658. https://doi.org/10.1177/0020702016684859
Hirst, M. 2015. Emerging Brazil: The Challenges of Liberal Peace and Global Governance. *Global Society* 29:3: 359 - 372. https://doi.org/10.1080/13600826.2015.1008422
Hochstetler, K. & M. Milkoreit 2015. Responsibilities in Transition: Emerging Powers in the Climate Change Negotiations. *Global Governance* 21:2: 205 - 226. https://doi.org/10.1163/19426720-02102003
Hofmann, S.C. & B.B. de Moraes Mendes & S. Campbell 2016. Investing in International Security: Rising Powers and Organizational Choices. *Cambridge Review of International Affairs* 29:3: 831 - 851. https://doi.org/10.1080/09557571.2016.1230593
Hopewell, K. 2014. Different Paths to Power: The Rise of Brazil, India and China at the World Trade Organization. *Review of International Political Economy* 22,2: 311-338. https://doi.org/10.1080/09692290.2014.927387
Hunt, C.T. 2016. Emerging Powers and the Responsibility to Protect: Non-linear Norm Dynamics in Complex International Society. *Cambridge Review of International Affairs* 29,2: 761 - 781. https://doi.org/10.1163/1875984X-00803007 https://doi.org/10.1163/1875984X-00803002
Hurrell, A. 2006. Hegemony, Liberalism and Global Order: What Space for Would-be Great Powers?' *International Affairs* 82,1: 1 - 19. https://doi.org/10.1111/j.1468-2346.2006.00512.x
Hurrell, A. 2010a. Brazil and the New Global Order. *Current History* 109,724: 60-66. https://doi.org/10.1525/curh.2010.109.724.60
Hurrell, A. 2010b. Brazil: What Kind of Rising State in What Kind of Institutional Order? In Alexandroff, A.S. & A.F. Cooper (eds.): *Rising States, Rising Institutions*. Washington, D.C.: Brookings Institution.
Ikenberry, G.J. 2008. The Rise of the China and the Future of the West – Can the Liberal System Survive? *Foreign Affairs* 87,1: 23 - 37.
International Commission on Intervention and State Sovereignty [ICISS] 2001. *Responsibility to Protect: Report of the International Commission on Intervention and State Sovereignty*. Ottawa: IDRC.
Job, B.L. 2016. Evolution, Retreat or Rejection: Brazil's, India's and China's Normative Stances on R2P. *Cambridge Review of International Affairs* 29:3: 891-910. https://doi.org/10.1080/09557571.2016.1208636

Jordaan, E. 2003. The Concept of a Middle Power in International Relations: Distinguishing between Emerging and Traditional Middle Powers. *Politikon* (Pretoria) 30, 2: 165 - 181. https://doi.org/10.1080/0258934032000147282

Jordaan, E. 2017. The Emerging Middle Power Concept: Time to Say Goodbye? *South African Journal of International Affairs* 24:3: 395 - 412. https://doi.org/10.1080/10220461.2017.1394218

Kacowicz, A.M. 2005. *The Impact of Norms in International Society: The Latin American Experience, 1881-2001*. Notre Dame: University of Notre Dame Press.

Kahler, M. 2013. Rising Powers and Global Governance: Negotiating Change in a Resilient *status quo*. *International Affairs* 89,3: 711 - 729. https://doi.org/10.1111/1468-2346.12041

Kelly, M. 2013. Fighting for their Lives: R2P, RwP and the Utility of Force to Protect Civilians. In Hamann, E. & R. Muggah (eds.): *Implementing the Responsibility to Protect: New Directions for International Peace and Security*. Brasília: Instituto Igarapé.

Kenkel, K.M. 2010. South America's Emerging Power: Brazil as Peacekeeper. *International Peacekeeping* 17,5: 644 - 661. https://doi.org/10.1080/13533312.2010.516958

Kenkel, K.M. 2012. Brazil and R2P: Does Taking Responsibility Mean Using Force? *Global Responsibility to Protect* 4,1: 3 - 29. https://doi.org/10.1163/187598412X619649

Kenkel, K.M. 2013a. 'Brazil'. In Bellamy, A.J. & P.D. Williams (eds.): *Providing Peacekeepers. The Politics, Challenges, and Future of United Nations Peacekeeping Contributions.* Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199672820.003.0016

Kenkel, K.M. 2013b. Brazil's Peacebuilding in Africa and Haiti. *Journal of International Peacekeeping* 17,3/4: 272 - 292. https://doi.org/10.1163/18754112-1704006

Kenkel, K.M. 2013c. Out of South America to the Globe: Brazil's Growing Stake in Peace Operations. In Kenkel, K.M. (ed.): *South America and Peace Operations: Coming of Age*. London: Routledge. https://doi.org/10.4324/9780203071502

Kenkel, K.M. & F. De Rosa Miranda 2015. Localization and Subsidiarity in Brazil's Engagement with the Responsibility to Protect. *Global Responsibility to Protect* 7,3/4: 325 - 349. https://doi.org/10.1163/1875984X-00704006

Harig, C. & K.M. Kenkel 2017. Are Rising Powers Consistent or Ambiguous Foreign Policy Actors? Brazil, Humanitarian Intervention and the 'Graduation' Dilemma. *International Affairs* 93,3: 625 - 641. https://doi.org/10.1093/ia/iix051

Kenkel, K.M. & M. Trote Martins 2016. Emerging Powers and the Notion of 'international responsibility': Moral Duty or Shifting Goalpost? *Brazilian Political Science Review* 10,1: n.p. https://doi.org/10.1590/1981-38212016000100003

Kenkel, K.M. & C. Stefan 2016. Brazil and the 'responsibility while protecting' Initiative: Norms and the Timing of Diplomatic Support. *Global Governance* 22,1: 41-78. https://doi.org/10.1163/19426720-02201004

Laïdi, Z. 2012. BRICS: Sovereignty, Power, and Weakness. *International Politics* 49:5: 614 - 632. https://doi.org/10.1057/ip.2012.17

Lipton, M. 2017. Are the BRICS Reformers, Revolutionaries, or Counter-revolutionaries? *South African Journal of International Affairs* 24,1: 41 - 59. https://doi.org/10.1080/10220461.2017.1321039

Lopes, D.M., G. Casarões & C.F. Gama 2013. A Tragedy of Middle Power Politics: Traps and Contradictions in Brazil's Quest for Institutional Revisionism. Paper presented at the Annual Convention of the International Studies Association, San Francisco.

Malamud, A. 2011. A Leader without Followers? The Growing Divergence between the Regional and Global Performance of Brazilian Foreign Policy. *Latin American Politics and Society* 53:3: 1 - 24. https://doi.org/10.1111/j.1548-2456.2011.00123.x

Mares, D.A. & H.A. Trinkunas 2016. *Aspirational Power: Brazil on the Long Road to Global Influence*. Washington, D.C.: Brookings Institution Press. https://doi.org/10.5771/9780815727965

Mattos, B.R.B., F.E. Lemos de Matos & K.K. Kenkel 2017. Brazilian Policy and the Creation of a Regional Security Complex in the South Atlantic: Pax Brasiliana. *Contexto Internacional* 39,2: 593-609. https://doi.org/10.1590/s0102-8529.2017390200004

Mello e Souza, A. de & P. Miranda (eds.). 2015. *Brasil em Desenvolvimento 2015: Estado, Planejamento e Políticas Públicas*. Brasília: Instituto de Pesquisa Econômica Aplicada (IPEA.

Milani, C.R.S., L. Pinheiro & M.R. Soares de Lima 2017. Brazil's Foreign Policy and the 'graduation dilemma''. *International Affairs* 93:3: 585-605. https://doi.org/10.1093/ia/iix078

Mitzen, J. 2011. Governing Together: Global Governance as Collective Intention. In Bjola, C. & M. Kornprobst (eds.): *Arguing Global Governance: Agency, Lifeworld and Shared Reasoning*. London: Routledge.

Moreno, M.F., C.C.V. Braga & M.S. Gomes 2012. Trapped between Many Worlds: A Post-colonial Perspective on the UN Mission in Haiti (MINUSTAH). *International Peacekeeping* 19:3: 377-392. https://doi.org/10.1080/13533312.2012.696389

Narlikar, A. 2011. Is India a Responsible Great Power? *Third World Quarterly* 32,9: 1607-1621. https://doi.org/10.1080/01436597.2011.619880

Nel, P. 2010. Redistribution and Recognition: What Emerging Regional Powers Want. *Review of International Studies* 36: 951-974. https://doi.org/10.1017/S0260210510001385

Neves, G.M.S. 2010. *Comissão das Nações Unidas para Consolidação da Paz- - Perspectiva Brasileira*. Thesis. Instituto Rio Branco. Brasília: Fundação Alexandre de Gusmão.

Patrick, S. 2010. Irresponsible Stakeholders? The Difficulty of Integrating Rising Powers. *Foreign Affairs* 89:6: 44-53.

Pu, X. 2012. Socialisation as a Two-way Process: Emerging Powers and the Diffusion of International Norms. *Chinese Journal of International Politics* 5: 341-367. https://doi.org/10.1093/cjip/pos017

Puri, H.S. 2016. *Perilous Interventions: The Security Council and the Politics of Chaos*. New York: HarperCollins.

Ralph, J. & J. Gifkins 2017. The Purpose of United Nations Security Council Practice: Contesting Competence Claims in the Normative Context Created by the Responsibility to Protect. *European Journal of International Relations* 23,3: 630 - 653. https://doi.org/10.1177/1354066116669652 PMid:29278256 PMCid:PMC5732619

Richmond, O. 2006. The Problem of Peace: Understanding the 'liberal peace'. *Conflict, Security and Development* 6,3: 291 - 314. https://doi.org/10.1080/14678800600933480

Risse, T., S.C. Ropp & K. Sikkink (eds.). 2013. *The Persistent Power of Human Rights: From Commitment to Compliance*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781139237161

Seabra, P. 2016. Defence Cooperation between Brazil and Namibia: Enduring Ties across the South Atlantic. *South African Journal of International Affairs* 23,1: 89-106. https://doi.org/10.1080/10220461.2016.1152910

Shesterinina, A. 2016. Evolving Norms of Protection: China, Libya and the Problem of Intervention in Armed Conflict. *Cambridge Review of International Affairs* 29,3: 812 - 830. https://doi.org/10.1080/09557571.2016.1170103

Solingen, E. 2012. Of Dominoes and Firewalls: The Domestic, Regional, and Global Politics of International Diffusion. *International Studies Quarterly* 56:4: 631 - 644. https://doi.org/10.1111/isqu.12034

Stefan, C.G. 2016. On Non-Western Norm Shapers: Brazil and the Responsibility while Protecting. *European Journal of International Security* 2,1: 88 - 110. https://doi.org/10.1017/eis.2016.18

Stochero, T. 2017. Brasil encerra participação na missão de paz da ONU no Haiti. G1 (Globo. 1 September 2017.) Available at: https://g1.globo.com/mundo/noticia/brasil-encerra-participacao-na-missao-de-paz-da-onu-no-haiti.ghtml (Accessed on 04 March 2018.)

Stolte, C. 2015. *Brazil's Africa Strategy: Role Conception and the Drive for International Status*. Houndsmills: Palgrave MacMillan. https://doi.org/10.1057/9781137499578

Stuenkel, O. & M.M. Taylor 2015. Brazil on the Global Stage: Origins and Consequences of Brazil's Challenge to the Global Liberal Order. In Stuenkel, O. & M.M. Taylor (eds.): *Brazil on the Global Stage: Power, Ideas, and the Liberal International Order*. Houndsmills: Palgrave MacMillan.https://doi.org/10.1057/9781137491657

Stuenkel, O. 2016. Brazil and Responsibility to Protect: A Case of Agency and Norm Entrepreneurship in the Global South. *International Relations* 30:3: 375 - 390. https://doi.org/10.1177/0047117816659594

Thakur, R. 2011. *The Responsibility to Protect: Norms, Laws and the Use of Force in International Politics*. London: Routledge. https://doi.org/10.1080/0163660X.2013.791082

Thakur, R. 2013. R2P after Libya and Syria: Engaging Emerging Powers. *Washington Quarterly* 36,2: 61-76.

United Nations General Assembly 2005. World Summit Outcome. 24 October. United Nations Document A/RES/60/1.

United Nations Secretary General 2009. Implementing the Responsibility to Protect. Report of the Secretary General. 12 January. United Nations Document A/63/677.

Uziel, E. 2016. 'Três questões empíricas, uma teórica e a participação do Brasil em operações de paz das Nações Unidas'. *Política Externa* 4,4: 91 - 105.

Vaz, A.C. 2015. Brazilian Approaches to Maritime Security Cooperation in IBSA and the Prospects for an Atlantic-Indian Maritime Security Governance. *Journal of the Indian Ocean Region* 11,2: 170 - 183. https://doi.org/10.1080/19480881.2015.1067382

Veja 2018. Gestão Bolsonaro evitará acordos comerciais com a 'mulambada', diz Mourão**.** Leia mais em: https://veja.abril.com.br/politica/gestao-bolsonaro-evitara-acordos-comerciais-com-a-mulambada-diz-mourao/

Wiener, A. 2009. Enacting Meaning-in-use: Qualitative Research on Norms and International Relations. *Review of International Studies* 35,1: 175 - 193. https://doi.org/10.1017/S0260210509008377

Wiener, A. 2014. *A Theory Contestation.* London: Springer. https://doi.org/10.1007/978-3-642-55235-9

Kai Michael Kenkel
Associate Professor
Institute of International Relations
Pontifical Catholic University of Rio de Janeiro
Rio de Janeiro
Brazil

Associated Researcher
German Institute of Global and Area Studies
Hamburg (GIGA)
kenkel.iri@gmail.com

# THE 2024
# BRICS
# SECURITY & ECONOMY
# NEXUSES CONFERENCE

# Chapter 7: The Use of the Internet for Nefarious Security Purposes: Policies, Developments and Challenges of Terrorist Content on Social Media[1]

**Nirmala Devi Gopal**
**ORCID iD: https://orcid.org/0000-0002-5104-0083**

## Abstract

This research is a non-systematic desktop literature review that draws on publicly available sources and aims to provide recommendations to civil society, academic researchers, and policymakers tasked with combatting terrorist content on social media. First, investigating the United Nations (UN) policy mechanisms by which members engage in counterterrorism and combatting terrorist narratives. Second, the research outlines the BRICS approach to combatting terrorism on social media through the lens of the last five (5) summit declarations, taken at the 10th to the 14th BRICS Summits from (2018 to 2022). Next, the research investigates terrorist's use of social media and the response from private companies to reduce terrorist content on their platforms. Last, the research investigates how journalists and civil society are impacted by broad bans of terrorist content on social media by drawing on the case of an East African journalist. The research found that while the UN, BRICS and private companies combat terrorism through policy mechanisms and the development of technology, broadly banning terrorist content on social media can inadvertently intersect with journalists and civil society actors. The research recommends that restrictions on terrorist content on social media should offer protection to journalists and civil society who may share content without the intention to incite violence.

[1] The author gratefully acknowledges the support of Wade Jenson Dayal, towards the production of this manuscript. (Editor.)

**Keywords:** BRICS, United Nations, violent extremism, terrorism, counter-terrorism, social media, journalism, civil society.

## 1 Introduction

Terrorism is a complex topic, with many nuanced implications in the current setting of a post-pandemic world and the present geopolitical and security climate. The involvement of terrorism as a nefarious activity on the internet and social media is a growing cause for concern. There are significant implications for the activities of countries, states, private companies, or civil society regarding the producers, regulators, and users of social media platforms (Gaswaga 2013: 17) aptly criticized that one's freedom fighter, is another's terrorist.

A careful discussion of this topic must begin by defining terrorism. As such, the researcher selected three (3) relevant definitions of terrorism drawn from open sources – first, a front-facing definition from the UN, as an authoritative source free of technical jargon. Second, a definition is written by an officially appointed representative of the UN while fulfilling their official duties at the time. Finally, a definition of terrorism initially codified by the United Nations (UN) in (2006 is presented, as it is part of an essential international counter-terrorism policy). All three (3) definitions are shown below and can be used interchangeably in this research to create a relevant understanding best suited to the level of abstraction necessary.

*First*, according to the online frontpage of the UN Office of the High Commissioner for Human Rights[2], 'terrorism involves the intimidation or coercion of populations or governments through the threat or perpetration of violence [that] may result in death, serious injury or the taking of hostages'.

*Second*, Aoláin (2018: 4 - 5), the UN Special Rapporteur for Counter Terrorism and Human Rights, recommended in a public letter addressed to Mr Zuckerberg M[3]. that the definition of terrorism relevant to the action or should encompass any action or attempted action, which violates regional or international law, and constituting any one or more of 'the taking of hostages, causing death or bodily harm to the general population, or any lethal or grievous physical violence to the general population'. Furthermore, Aoláin (2018: 4-5)

[2] An online series focusing on terror and violent extremism. Available at: https://www.ohchr.org/en/topic/terrorism-and-violent-extremism

[3] In a 2018 letter addressed to Mr M. Zuckerberg, about the appropriate definition of 'terrorism' in the context of online social media.

states that the best practice for the offence of terrorist incitement as 'an offence to intentionally and unlawfully distribute or otherwise make available a message to the public with the intent to incite the commission of a terrorist offence, where such conduct, whether or not expressly advocating terrorist offences, causes a danger that one or more such offences may be committed'. In simpler terms, terrorism is defined as any one or more of the above three (3) points raised by Aoláin (2018: 4-5), which pertain to any actions intending to incite further illicit acts, especially if there is a real risk of such events.

*Third*, the UN General Assembly adopted the *United Nations Global Counter-Terrorism Strategy*[4] *UNGCTS) UNGA (2006)* on 8 September (2006). The UNGCTS is a living document encompassing a comprehensive, collaborative, ongoing international approach to condemn and combat terrorism. In simple terms, the UNGCTS is the primary counter-terrorism international policy created by the UN. It is periodically updated, though the current version being discussed is its earliest incarnation or edition. The most recent edition of the UNGTCS is discussed later. The UNGCTS describes 'terrorism' as comprising or constituting any action or activity that may bring destruction to 'human rights, fundamental freedoms and democracy, threats to the territorial integrity and security of States, and, destabilising legitimately constituted Governments'.

In descending order, the above three (3) definitions represent a terrorism concept that ranges from general to more specific. There can be no dispute that terrorism is a crime and brings grave harm to both states and civilian populations, as well as the theme of avoiding any harm to human rights. In conjunction with threatening the security and wellbeing of states, civil society, and human rights, terrorism has increasingly become intertwined with emerging technological threats, as described below.

The word 'incite' and its related terms appear approximately twenty-two (22) times in this research, as it is a necessary component of defining the term 'terrorism'. To this end, Articles 25 and 28, respectively, of the United Nations *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*[5] call for narrowing the 'the terms of the crime of incitement'. The former points to general conditions. The latter article points to three (3) conditions that must be

[4] Res. *A/RES/60/288.* The United Nations Global Counter Terrorism Strategy UNGCTS. Available at: https://undocs.org/A/RES/60/288

[5] Res. *A/61/267:* Available at: https://undocs.org/A/61/267

satisfied in order to narrowly define the crime of incitement, namely 'the intent to incite the commission of a terrorist offence, that this intent is not of one or several individuals, but the will of an association, group or political party, and, there must exist a real risk that such acts may take place'.

In October 2022, the UN Security Council Counter-Terrorism Committee unanimously adopted the Delhi Declaration, '*Countering The Use of New and Emerging Technologies for Terrorist Purposes*'. The Delhi Declaration states that terrorism constitutes 'one of the most serious threats to international peace and security and that acts of terrorism are criminal and unjustifiable regardless of their motivations'. Furthermore, this declaration highlights emerging technological threats like 'increasing global misuse of unmanned aerial systems/vehicle UAS, UAV or 'drones') by terrorists for conducting attacks against, incursions into critical infrastructure and soft targets or public areas'. A UN (2022) online news article corroborates the focus on emerging digital security threats presented by the use of drones, social media, and cryptocurrencies in illicit terrorist activities. Through an open-source investigation, Haugstvedt (2024: 140) found that violent non-state actors VNSAs) were responsible for over 1,100 UAV attacks from (2006 to 2023) and that VSNAs 'choose targets discriminately and direct most of their UAV attacks against hard or hardened targets, such as military or hardened civilian targets'. The last-mentioned author challenges the view of the Declaration in terms of the targets of illicit drone attacks critical infrastructure, soft targets, or public areas vs hardened targets like the military. Accordingly, it is due to economies of scale, which reward innovation and mass adoption, lower prices, and make technology like drones, increasingly available for any licit or illicit use.

In a digital post-pandemic age, equal concern must be given to the activities of violent extremist and terrorist organisations, which have increasingly radicalised new members recruited and disseminated propaganda via the internet and social media. This research is a desktop literature review that draws on publicly available online sources, academic literature, and reports. It aims to provide general recommendations to policymakers to combat terrorist content on social media. *First*, the research outlines the most important UN policy mechanisms by which members can engage in counterterrorism and combatting terrorist narratives. *Second*, the research outlines the BRICS approach to combat terrorism on social media through the lens of the last five (5) summit declarations, taken at the 10th to the 14$^{th}$ BRICS Summits from (2018 to 2022). Next, the research investigates terrorism on social media and examines the response of private companies to reduce terrorist content on their

platforms. *Last*, the research investigates how journalists and civil society actors can be impacted by broad bans of illicit content on social media. The research targets policymakers, scholars, and stakeholders concerned with developing or implementing policies to limit terrorist content on social media.

## *1.1 Problem Statement*

The problem addressed in this research is the knowledge-gap created by the lack of general understanding and awareness around the topic of terrorism, combatting terrorist narratives, and the implications of terrorist content on social media. This problem necessitates a careful investigation and review of relevant policies of the UN and BRICS, the responses of private companies, and a discussion of real-world problems, which this research aims to address. This research aims to address the problem by investigating and describing relevant policies of the UN and BRICS, as well as the responses of private companies.

Furthermore, the research seeks to provide additional insight into the impact of broadly banning illicit content on social media by focusing on a real-world case study, highlighting essential implications for the broader security community. While private companies use many effective methods for reducing terrorist content on social media, many nuanced sub-problems arise from strict policies, especially during heightened risk.

## *1.2 Aim*

The present research aims to provide general recommendations to policy-makers, scholars and stakeholders concerned with developing or implementing policies to limit terrorist content on social media.

## *1.3 Objectives*

To achieve this aim, the research objectives are to:

(i) To outline the policy mechanisms of the UN by which members of the General-Assembly can engage in counterterrorism and the combatting of terrorist narratives;

(ii) To outline the BRICS approach to combatting terrorism on social media

through the lens of the last five (5) summit declarations, taken at the 10th to the 14th BRICS Summits from (2018 to 2022);

(iii) To investigate terrorists use of social media and examine the response of private companies to cooperate in reducing terrorist content on their platforms; and,

(iv) To investigate how journalists and civil society actors are impacted by broad bans of terrorist content on social media by drawing on the case of a journalist from East Africa.

## *1.4 Research Questions*

To satisfy the above objectives, the researcher specifies the following research questions:

(i) What are the policy mechanisms of the UN that members use to engage in counterterrorism and combatting terrorist narratives?

(ii) What is the BRICS approach to combatting terrorism on social media through the lens of the last five (5) summit declarations?

(iii) Why do terrorists use social media, and what are private companies doing to reduce terrorist content on their platforms?

(iv) Case study: how do broad bans of terrorist content on social media impact journalists and civil society?

## *1.5 Rationale*

Despite successes of international policies, cooperative efforts of government and private industry, and technology aimed at combating the issue of terrorist content on social media, ongoing terrorist operations on social media present a problem, especially involving narratives which aim to recruit, radicalise, or incite violence.

The challenge lies in the often-conflicting interests of states and civil society, where the latter may distribute digital content deemed offensive by the

former. As a result, policymakers must strike a balance between addressing the issue of terrorist content on social media without stifling the positive effect of counter-terror narrative-related content that journalists and civil society may contribute. Investigating this topic area is precarious but can be conducted with sufficient caution. There is an opportunity to learn from other contexts and contribute to the topics of counter-terrorism and illicit uses of social media using open-source investigative techniques (OSINT).

To sufficiently address the research questions above, the researcher will use OSINT techniques and their judgement and experience navigating online resources to target critical data sources more efficiently. Therefore, the above rationale of this research is comprised of a general awareness that the topic of terrorist content on social media is complex, that there is a need for the careful balancing of policies, and an imperfect willingness to learn from other contexts.

## 2 Methodology

Salkind (2010: 799 - 800) states, 'the methods section should provide a clear and precise description of how a study was done and the rationale for the specific procedures chosen'. Furthermore, it must contain enough information to i) repeat the study and ii) independently verify the validity of the results and conclusion of the research. Therefore, the methodology is primarily an opportunity to be transparent about the methods, tools, and decisions regarding how and why choices are made while conducting research. This is the primary purpose of the methodology.

In practising the transparency mentioned above, the researcher recognises that bias is inevitable. Many of the methods described below inevitably lead to one form of bias or another, and there can be no shying away from it. However, bias can be controlled, managed, and minimized by being transparent, triangulating sources, and repeating or cross-referencing topics. This is the second purpose of the methodology.

Data collection consists of searching for relevant data sources or literature online. The researcher performs keyword searches using online search engines, develops research ideas and manages data during this period. Initially, the focus was to explore the broader topic of terrorism and develop broad research objectives. Before long, the focus shifts to specifying more explicit objectives and research questions while targeted literature is gathered to address those questions.

## *2.1 Literature Review as a Research Methodology*

This research uses literature review as a methodology. The researcher chose purposive and convenience sampling as non-probability sampling techniques. This methodology is not systematic; instead tries to explore he topic area and present balanced arguments. This research positions the researcher as 'an 'instrument' in the process' and is unobtrusive, used to study aspects of social behaviour without attempting to make changes or influence it. Literature review ultimately benefits from the static nature of published documents.

In simple terms, the researcher searches for and reads data, deciding whether it is relevant to answering a research question. Whether the data is included through an in-text reference and may include a direct quote, a paraphrased section, and a reference list.

The first and second research questions describe the UN and BRICS policies on terrorism, terrorist narratives, and social media. The third question investigates how and why terrorists use social media, in contrast to some preventive steps the largest Western social media companies have committed. Significant online media and public attention surrounds the journalist's arrest, which warrants further investigation. This led to the development of the final question, which seeks to highlight lessons and pitfalls of how broad bans of terrorist content on social media may impact journalists and civil society.

The first data source collected is a review titled 'Open Source Intelligence OSINT): Issues and Trends'. Three months later, the final data source collected is a situational report about terrorism and the activities of military forces in the Federal Republic of Somalia 'Somalia'), East Africa. The researcher engaged with new material daily, wrote an initial draft, and presented it to peers. The careful review, reflection, and streamlining of all efforts led to the creation of this research.

## *2.2 Ethical Open-Source Intelligence (OSINT) Gathering*

The 'source data or literature' ('data') collection period lasted approximately three (3) months. Open Source INTelligence (OSINT) gathering can support many types of data collection procedures for various purposes and comes with benefits and drawbacks. Some recent exciting examples of OSINT in academic security research include Yeboah-Ofori (2018), titled 'Developing Mitigation Techniques Against Cybercrime Threats on Social Media', and Senekal and Kotzé (2019), titled 'OSINT for Conflict Monitoring in Contemporary South

Africa: Challenges and Opportunities in a Big Data Context', among others. When used within reason and ethical boundaries, OSINT can be a powerful research tool.

In this research context, OSINT is used to explore and collect only ethically sourced information available through non-systematic search online. This includes the UN policies, BRICS declarations, government media statements, reports, and publicly available documents. If it is reasonably intended for public consumption or academic debate, it is widely reported online and does not include any sensitive or personal information from unethical sources. These sources are not typically available through conventional academic databases.

The web browsers used in this research are Chrome and Tor. The benefit of using multiple browsers is not to repeat every search but to test the accessibility of unclear ones. An important example is to test whether a source URL is freely accessible when directly requested instead of passed on from the primary search engine. Targeted keyword searches are performed for each research question. Duplicate, irrelevant, and poor-quality results are ignored.

## *2.3 Non-systematic Keyword Searching, Referencing, and Web-archiving Techniques*

Zanasi and Ruini (2018: 441 - 442) describe keyword searching as a valuable tool for analysts but warn about preconceived notions or existing beliefs, and rightfully so. Algorithmic bias is a severe concern for research integrity. However, there is an opportunity for novice researchers to approach new topics in complex research areas and, later, target or triangulate specific concepts by leveraging the power of advanced indexing technology to find more relevant information using techniques like keyword searching. Researchers using keyword techniques must be guided by a strong sense of morality, abide by the copyright rules, and respect for the source material.

First, the referencing style used in the research complies with the approved UKZN (2020) APA-7 referencing style guide and is further modified to suit he publication's style guide. Referencing is an important skill which contributes to avoiding plagiarism. Data sources or literature are recorded and managed using Endnote reference management software. Its implementation includes in-text references and a complete reference list at the close of this research.

Second, to address future availability and enable auditing, the researcher created public web caches of individual reference links – a snapshot of a website or web content when allowed by the website owner only. The importance is placed on functionality, utility, and ease of use of the Internet Archive's Wayback Machine 'save page now' feature, accessible at: https://web.archive.org/save.

The choice to use this service provider over another is based on the researcher's experience. Web archiving (or 'web-caching') content creates a pseudo DOI, lending some permanence to online public sources, especially those that lack perma-links or Digital Object Identifiers DOIs. These public caches created for this research are accessible at: https://archive.org/details/@wade_jenson_dayal?tab=web-archive.

For research purposes, using web archiving to preserve or access online information hinges on respecting the legitimate wishes of website administrators or owners – who may decide to prevent all caching activity to protect copyright work or for any other reason. Such wishes are respected in all cases, and no further attempts are made. The researcher initiates the archiving, but its activity is automatic - and strictly for only non-profit, educational, and public archiving purposes.

## *2.4 List of Initial Keywords*

The keywords below were used to find the source data. The search is not systematic. Keywords were combined and formed into phrases or sentences to target more relevant sources.

- **RQ1:** United Nations; United Nations AND Counterterrorism; United Nations AND Counter-Terrorism UNGCTS); United Nations AND Sanctions; United Nations AND Violent extremism; United Nations AND Terrorist narratives; United Nations AND Terrorism AND Human rights.

- **RQ2:** BRICS; BRICS AND Summit declaration per year); BRICS AND Information Communications Technologies ICTs); BRICS AND Terrorism; BRICS AND Terrorism AND Social media

- **RQ3:** Terrorism AND United Nations AND Social media; Terrorism AND Social media platform names: Youtube; Meta/Facebook; X

formerly 'Twitter'); Terrorism AND Social networks; Terrorism AND Social networks AND Extremism; Terrorism AND Social networks AND Online recruitment; Terrorism AND Al Shabaab AND Social media; Terrorism AND Redirect method; Terrorism AND Meta hasher matcher; Terrorism AND Private companies.

- **RQ4:** Terrorism AND Africa; Terrorism AND Africa AND countries; Terrorism AND African Union AU); Terrorism AND Somalia; Terrorism AND Somalia AND Social media: Terrorism AND Somalia news report; Terrorism AND Somalia AND Journalism; Terrorism AND AMISOM; Terrorism AND ATMIS; Terrorism AND Somalia Government report; Terrorism AND content ban; Terrorism AND Counter-narrative; Terrorism AND Somalia AND Journalist.

## 3 Review of the Literature

This research section constitutes the results of the non-systematic literature review. The section is structured as summarised responses to each of the research questions.

### *Q1: What are the Policy Mechanisms of the UN that Members Use to Engage in Counterterrorism and Combatting Terrorist Narratives?*

This section addresses the question above, which asks what the policy mechanisms members of the UN use to engage in counterterrorism and combatting terrorist narratives. The data used for this section includes international policy documents, research, electronic documents, and public sources. The main focus is on specific UN strategies, plans, and resolutions. This section briefly considers 'What is the UN?', and 'what policy mechanisms do members use to engage in counter-terrorism and terrorist narratives?'.

The UN (2023b) was formed in 1945 and self-describes as being composed of six (6) bodies or organisations, as described next. This includes the General Assembly UNGA), which consists of all 193 member states. Second, the *Security Council* UNSC), a focused body made up of permanent and rotating members, maintains international peace and security. Third, the *Economic and Social Council*, promotes international economic cooperation.

Fourth, the Trusteeship Council is currently suspended. Fifth, the *International Court of Justice*, acts as the judicial arm of the UN. Sixth is the *UN Secretariat*, which carries out the UN's work via the Secretary-General. Members of the UNGA may engage in counter-terrorism and combatting terrorist narratives through the full scope of UN policy mechanisms or the UNSC in particular.

First, adopted in (2006, the *United Nations Global Counter-Terrorism Strategy* (UNGCTS), its review updates as mentioned, and supporting the UNGA and Security Council's resolutions and decisions, is a policy mechanism which members of the UN can use to engage in counterterrorism. The UNGCTS supports combatting terrorism through four (4) pillars. First, through addressing the conditions conducive to the spread of terrorism. Second, implementation of measures to prevent and combat terrorism. Third, increasing states' capacity to prevent and combat terrorism and strengthening the UN system's role for this purpose. Last, to ensure respect for human rights and the rule of law, as the fundamental basis of the fight against terrorism.

According to a report by the Global Center on Cooperative Security, the first (1st) critical innovation of the Strategy is the emphasis on preventative measures, and the second (2nd) innovation involves reframing the link between human rights and counterterrorism – as mentioned in the fourth (4th) pillar of the UNGCTS, shown above. According to this report of the GCCS (2020: 8):

> The Strategy UNGCTS) enshrines the importance of civil society engagement as part of a 'whole of society' approach to prevent and counter violent extremism and terrorism, highlighting the determination of member states to encourage their engagement 'as appropriate' on efforts to implement the Strategy. The international community has more specifically recognized the role of civil society in this space to be appropriate in the development of national Preventing Violent Extremism (PVE) plans of action, the rehabilitation and reintegration of foreign fighters, and efforts to counter terrorist narratives.

The UNGA adopted the seventh review of the UNGCTS[6] on 2 July (2021). The seventh review of the UNGCTS reflects the latest declaration of intent of the UN about effectively reducing terrorism. Within it, the UNGA (2021: 4) stressed 'the importance of the role of the media, civil society, religious actors, the business community and educational institutions in efforts to enhance

[6] Res. A/RES/75/291. Available at: https://undocs.org/A/RES/75/291

dialogue and broaden understanding, in promoting pluralism, tolerance and coexistence, and in fostering an environment which is not conducive to incitement of terrorism, as well as in countering terrorist narratives'. Furthermore, as stated in the seventh review, members called for a safer ICT space and addressed the increased involvement of the internet with terrorism and other media, among others. The above shows that the UN is committed to combatting terrorism and recognises both the need for safer ICTs and the critical role played by members of civil society.

The seventh review of the UNGCTS strictly condemns the recruitment of children for terrorism, including abuse and use of children to commit violent attacks. In particular, the children's roles in conflict were recognised in Articles 47, 53, 113, and 117, respectively. First, Article 47 pertains to the use of children as foreign fighters. Second, Article 53 pertains to the UN's call for the protection and rehabilitation of children. Third, Article 113 deplores the suffering brought to women, children and their families arising from terrorism, wherein the UNGA recognised sexual violence at the hands of terrorists. Last, Article 117 pertains to the UNGA call for states to consider alternatives to punishment, prosecution, or detention that may be given to recruited children.

The specific question of how members of the may combat terrorist narratives concerning the seventh review of the UNGTCS is best addressed in Articles 16, 20, 21, 22, and 24, among others. In order, the articles above are summarised as i) considering more accurate depictions of terrorist recruitment, ii) working with private companies, iii) public policing of online spaces and the identification of misrepresentations, iv) the use of historical illicit content, and, v) through regional approaches.

Second, members engage in counter-terrorism through '*The Plan of Action to Prevent Violent Extremism*'[7] 'the plan'). Generally, the plan aimed to combat violent extremism as it creates conditions conducive to terrorism. The plan constitutes a three-point system to combat violent extremism, including:

(i) the creation of necessary counter-terrorism frameworks at all levels, and includes strategically mobilising resources aimed at preventing further terrorist activities in future;

(ii) taking action against violent extremism; and,

[7] Plan. *A/70/674.* Plan of Action to Prevent Violent Extremism. Available at: https://undocs.org/A/70/674

(iii) providing necessary support to members and local communities through the United Nations by creating inclusive approaches that aim to develop the capacity of members.

In order to 'take action' as mentioned above, the plan engages critical intersection with several UN Sustainable Development Goals SDGs), including opening dialogues and preventing conflict, bolster governance, access to human rights and the rule of law, drive community engagement, bring empowerment to youth, women and gender equality, improve education, skills development, and employment, and, improve communications, the internet, and social media. In other words, engagement with the plan of action to prevent violent extremism can be achieved by implementing the UN sustainability goals.

If such goals are to be attained, and the plan of action to prevent violent extremism is to succeed in relevant cases), then the underlying conditions or drivers preventing their attainment must be delineated. To this end, the plan specifies underlying drivers and conditions that create the conditions for violent extremism to thrive in society, including a lack of socioeconomic opportunities, widespread marginalisation and discrimination, poor governance, severe violations of human rights and the rule of law, prolonged exposure to conflict, and a lack of a resolution to such conflict, and, the radicalisation of persons in correctional services facilities, like prisons.

Third, the United Nations Security Council UNSC) later adopted the '*Comprehensive International Framework to Counter Terrorist Narratives*'[8] in 2017, which aims to counter terrorism by diminishing terrorist narratives and promoting positive narratives. According to the UNSC (2017a: 2 - 7), the core framework to counter terrorist narratives is comprised of three (3) elements, including 'legal and law enforcement measures per obligations under international law and consistent with United Nations resolutions', 'public-private partnerships', and, 'the development of counter-narratives'. Additionally, the framework to counter terrorist narratives, as above, is recognised by the UN Security Council in Resolution 2354[9], wherein it is stressed that:

(i) Countering terror narratives must take into account the principles of respecting the sovereignty, territorial integrity and political indepen-

[8] International framework. *S.2017/375*. Comprehensive international framework to counter terrorist narratives. Available at: https://undocs.org/S/2017/375
[9] Res. *S/RES/2354 2017.* Available at: https://undocs.org/S/RES/2354 (2017)

dence of all States in Article 2 (a);

(ii) efforts to counter terrorist narratives can benefit from engaging with various civil society actors, such as youth, families, women, religious, cultural and educational leaders, and other members of civil society, in Article 2 (f); and,

(iii) counter-terror narratives should go beyond a rebuttal of terrorist narratives, provide credible alternatives, and address the issue of vulnerable audiences subjected to terrorist narratives in Article 2 (j).

.

Fourth, counter-terrorism occurs through mutual engagement with subsidiary bodies of the UNSC, including committees like the Counter-Terrorism Committee CTC), the Counter-Terrorism Executive Directorate CTED), the UNOCT, the UN Counter-Terrorism Centre UNCCT), working groups that aim to support coordinating efforts to combat terrorism at all levels. Additionally, a repository of relevant legal instruments, including conventions, protocols, treaties, resolutions, and regional instruments, penned by the Special Rapporteur on Counter-Terrorism and Human Rights, titled *International Standards on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, and, all annual publishing's of the Special Rapporteur to the Human Rights Council HRC) and UNGA, are publicly available.

In addition to engagement with subsidiary bodies of the UN, economic or political sanctions are alternative tools to pressure terrorist organisations. The United Nations Department of Political and Peacebuilding Affairs describes sanctions as a focused tool for combatting terrorism, and typical criteria include threats to peace and security, violations of international humanitarian law, and wilfully obstructing humanitarian aid. Since 2004, sanctions regimes have taken a more focused approach to targeting specific individuals, entities, and groups, often restricting their travel, assets and through arms embargos. Therefore, in egregious cases of violent extremism or severe and ongoing terrorism acts, the UNSC may also establish sanctions to create cascading restrictions and compound pressure on terrorist and violent extremist groups.

In conclusion, members can use many UN policy mechanisms to counter-terrorism and combat terrorist narratives. More specifically, members of the UNGA may engage through the scope of UN policy mechanisms or other policy routes, like the UNSC. *First*, members engage through the *United*

*Nations Global Counter-Terrorism Strategy*[10] (UNGCTS), its review updates as mentioned, and supporting the UNGA and Security Council's resolutions and decisions. *Second*, members engage in counter-terrorism and combatting terrorist narratives through *The Plan of Action to Prevent Violent Extremism*[11]. The UNGA adopted the plan in 2015 and aimed to combat violent extremism as it becomes conducive to terrorism and terrorist activities. *Third*, the United Nations Security Council UNSC) later adopted the *Comprehensive International Framework to Counter Terrorist Narratives*[12] in 2017, which aimed to counter terrorism by diminishing terrorist narratives and promoting positive narratives. *Fourth*, members engage in counter-terrorism through mutual engagement with subsidiary bodies of the UNSC, including the CTC, CTED, UNOCT, UNCCT, and working groups, among others. Additionally, a repository of relevant legal instruments, including conventions, protocols, treaties, resolutions, and regional instruments, titled 'International Standards on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism', and all annual publishing of the Special Rapporteur to the Human Rights Council HRC) and UNGA, are publicly available OHCHR (2023a; 2023b).

## *Q2: What is the BRICS Approach to Combatting Terrorism on Social Media through the Lens of the Last Five (5) Summit Declarations?*

BRICS Declarations create significant political and economic implications for member countries by outlining mutual goals and principles to enhance cooperation and collaboration on trade, investment, and capacity building. Over the last five (5) years, BRICS Declarations increasingly connected with the themes of terrorism, the internet, and social media.

The data used in this section includes BRICS declarations from the 10th to the 14th BRICS Summits from 2018 to 2022. The data is sourced from respective domains of BRICS, as the publishers of the BRICS declarations. The

[10] United Nations Global Counter-Terrorism Strategy. https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy

[11] Plan. *A/70/674.* Plan of Action to Prevent Violent Extremism. Available at: https://undocs.org/A/70/674

[12] per *S/2017/375,* mentioned earlier. See footnote 9.

aim is to analyse each declaration's focus or relevance to combatting terrorism on social media.

In 2018, the 10th BRICS summit convened in Johannesburg, South Africa. The Johannesburg Declaration committed to future strategic cooperation and addressed the opportunities and challenges of the Fourth Industrial Revolution. The Johannesburg Declaration ratified members' commitment to condemn terrorism and recognised the internet's role in the potential misuse by terrorist organisations.

In 2019, the 11th BRICS summit convened in Brasilia, Brazil, under the theme '*BRICS: Economic Growth for an Innovative Future*'. *The Brasilia Declaration* reaffirmed members' commitment to condemn terrorism and engage in multilateral efforts to reduce it, stating that they 'recognise progress made in BRICS cooperation in counter-terrorism and welcome the results of the Fourth Meeting of the BRICS Counter-Terrorism Working Group'. In 2019, the BRICS Working Group on Counter-Terrorism constituted five smaller groups, each representing one of the following focus areas including '*terrorist financing*, *use of the internet for terrorist purposes*, *countering radicalization*, *limiting the issue of foreign terrorist fighters*, and *capacity-building*'.

In 2020, the 12th BRICS summit was convened virtually in Moscow, Russia. The summit's theme was '*BRICS Partnership for Global Stability, Shared Security, and Innovative Growth*'. The summit's conclusion saw the adoption of both *The Moscow Declaration* and the *BRICS Counter-Terrorism Strategy* CTS). The BRICS (2020b: 5) CTS represents the first recognition of the themes of terrorism, the internet and social media as: 'to counter extremist narratives conducive to terrorism and the misuse of the Internet and social media for terrorist recruitment, radicalisation and incitement and providing financial and material support for terrorists'.

In 2021, the 13th BRICS summit was convened virtually in New Delhi, India. The summit's theme was '*Intra BRICS Cooperation for Continuity, Consolidation, and Consensus*'. The conclusion of the summit saw the adoption of *The New Delhi Declaration*, which 'summarised the achievements of BRICS cooperation in various fields and expressed a common BRICS voice on strengthening cooperation in public health and vaccines, promoting world economic recovery, implementing the *2030 Agenda for Sustainable Development* and safeguarding world equity and justice'.

Additionally, the summit's conclusion also saw the adoption of the aligned BRICS 'Counter-Terrorism Action Plan' CTAP), which focused on the following areas of multilateral cooperation, including combatting terrorism,

preventing and countering radicalization, preventing and countering online threats, countering terrorism financing, preventing/curbing the travel of terrorists through border management, capacity building, protecting soft targets, information and intelligence sharing; and, international and regional cooperation.

The CTAP emphasized the need for a deep and ongoing investigation of the abovementioned mechanisms by which terrorists may use the internet and social media, emphasizing the State's role in response to the threat of terrorist narratives aimed at recruitment, radicalization, and incitement, especially of the youth. Furthermore, the CTAP encouraged a discussion of cooperation with private social media companies to reduce terrorist content on their services, specifically by 'blocking, filtering or removing content' and sharing details about the users posting illicit content. It also states that they can use social media to help inform law enforcement and criminal prosecution of terrorist activity.

In 2022, the 14th BRICS summit was held in Beijing, China. According to *The Beijing Declaration*, members reaffirmed their 'commitment to the promotion of an open, secure, stable, accessible and peaceful ICT environment'. Herein, members also exercised the importance of strengthening regional and multilateral cooperation to ensure the security of ICTs and Internet technology.

The Beijing Declaration states that members aimed to achieve this by 'advancing practical intra-BRICS cooperation through implementing the BRICS Roadmap of Practical Cooperation on ensuring security in the use of ICTs' and 'the activities of the BRICS Working Group on security in using ICTs'. In particular, BRICS (2022b) members committed to engaging with relevant working groups to meet the security goals of the previous year and intended to unify ICT security standards in future:

> We support the leading role of the United Nations in promoting constructive dialogue on ensuring ICT-security, including within the UN Open-Ended Working Group on the security of and in the use of ICTs 2021-2025, and developing a universal legal framework in this realm. We call for a comprehensive, balanced, objective approach to developing and securing ICT products and systems.

BRICS Declarations create significant political and economic implications for member countries by outlining mutual goals and principles to enhance cooperation and collaboration on trade, investment, and capacity building. Over the last five (5) years, BRICS Declarations increasingly connected with the

themes of terrorism, the internet, and social media. BRICS declarations are increasingly committed to combatting terrorism in its many forms, and they recognize new and emerging threats posed by the internet and communications technologies, including social media. Each declaration encompasses a greater recognition of the need to protect ICTs, the internet, and social media than the last.

## *Q3: Why do Terrorists use Social Media, and What are Private Companies Doing to Reduce Terrorist Content on their Platforms?*

This section is a literature review which seeks to address the above questions. In general, cheap and fast communication is helpful for every person in society, especially for nefarious purposes. The data used for this section includes international policy documents, research, electronic documents, and public sources, as mentioned. First, this review will focus on why terrorists use social media. Secondly, what are the most prominent social media companies doing to combat terrorist content online? At the end of addressing each sub-question, a summary list is presented.

## Why do Terrorists Use Social Media?

Sheik (2017: 14 - 15) stated that 'social media' can be viewed as an emergent digital technology that challenges the dominance of legacy media, whereby any individual can publish information and potentially reach a wide-ranging audience – ostensibly, at no cost to the individual. According to Hu and Yu (2021: 2), social media is an indispensable dimension of information and communications technologies ICTs), and typical ICT-based social media can be defined as any modern social aspect of the web that allows users to create and share user-generated content through email, blogs, instant messaging IM), social networks like Facebook, X formerly 'Twitter'), YouTube, other forums and online games. Ahmad (2022: 24 - 25) defined the term 'social media' as 'online tools allowing individuals and communities to communicate with each other; to share information, ideas, personal messages, images and other content, and where possible, collaborate in real-time and exchange ideas based on the data that they share'.

According to Hossain (2015: 5), terrorists use the internet for many

reasons, including 'operational communication, intelligence gathering, technical information sharing, recruiting, training'. According to Ucko (2018: 255), groups such as Al-Qaeda and ISIS have used the internet and social media to radicalise sympathisers, draw in new fighters to conflict zones and incite further attacks. From a political perspective, Chigudu (2021: 415) states that terrorism can be viewed as a revolutionary tactic by non-state actors who seek to disrupt governments and that terrorist groups thrive on disseminating extremist content on social media, aiming to indoctrinate and radicalize.

Klausen (2015: 17) found that 'Twitter was used for recruitment and indoctrination, as well as to build a transnational community for violent extremism'. In later research, Klausen (2016: 44 - 45) described a model of a terrorist network on social media as the 'star network structure', which is peer-based, decentralized, and driven by the desire to prioritize recruitment of new followers, as opposed to growing large online extremist communities. Furthermore, Klausen (2016: 48) states that 'opportunity, access and persuasion have all played a role in jihadist online recruitment'. Lastly, Klausen (2016: 49) states that the extremism on social media and in the real world blend into a vortex of contagion through the migration of both young men and women to the Islamic State as being supported by social media, which serves to bridge the separation between home life and a separate life of extremism.

A 2015 report by the Intergovernmental Authority on Development Security Sector Program stated that small terrorist networks, or 'cells', had become diffused while continuing to associate with Al-Shabaab and its affiliates – a terror and extremist group that will be investigated – and that one such terror cell was being monitored in Mombasa at the time, which engaged in an illicit activity primarily via social media and the internet. The IGAD SSP (2016: 30) report also states that via a social media analysis, this Mombasa-based cell had sought to procure explosives and operational facilities and discussed travel plans via coded messages on Facebook and X formerly 'Twitter'. Lastly, the IGAD SSP (2016: 31 - 32) report denotes the transnational threat posed by Al-Shabaab. Specifically, their attempts to recruit and radicalise young East African women, which builds and sustains transnational networks and routine travel through East Africa. Some illicit activities include the trafficking of explosives or other illicit dangerous materials across borders.

According to Cox *et al*. (2018: 2), al-Shabaab used social media for illicit activities, such as sharing propaganda, recruiting followers, and coordinating activities. This includes engaging with Twitter and YouTube users and remote video communications.

Research conducted by The United Nations Assistance Mission in Somalia found that the recruitment and messaging of Al-Shabaab targeted vulnerable youth, such as children between 10-15 years of age. Furthermore, they incentivized male children to join by providing protection, money, heightened status, essential resources like shelter, and promising young brides. The researchers describe that Al-Shabaab uses additional pressure tactics in recruitment, such as donating cell phones to youth and hosting small public gatherings. Furthermore, nearly all respondents in their research reported that Al-Shabaab relied on social media and radio frequencies to get its message out. In particular, the UNSOM (2017: 14) report raised five (5) main ways that Al-Shabaab facilitated the recruitment of new members, including *direct recruitment*, *forced recruitment*, *third-party recruitment*, *media publicity*, and *religious persuasion,* as described next. First, *direct recruitment* refers to targeting vulnerable groups like youth, women, and others through offering enticing incentives. Second, *forced recruitment* refers to the kidnapping or intimidation of people, including forcing parents to give up their children. Third, *third-party recruiting* refers to applying peer-pressure through third parties, such as extended family members or friends who are compromised. Fourth, *media publicity* refers to disseminating propaganda on social media, radio, or online. Fifth, *religious persuasion* refers to influence from radicalized religious leaders or teachers.

According to the United Nations Office on Drugs and Crime UNODC) '*Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System*' argued that while all children are tactically advantageous to terrorist and extremist groups, young girls may be more so, because they are more obedient and less noticeable, and as a result are often used as spies, messengers, and to undertake suicide bombings. This UNODC (2017: 11 - 13) handbook also states that terrorists and violent extremists use seven (7) strategies and tactics to recruit children, including *forcible recruitment*, *recruitment through ties between the group and community leadership*, *economic enticement*, *transnational recruitment*, *compromised education*, *dissemination of propaganda*, and *online recruitment*, as summarised next. *First*, *forcible recruitment* is described as kidnapping, abduction, or coercion of vulnerable children. *Second*, *recruitment through social ties* is described as peer-pressure from radicalized families and community leaders who may coerce children to join. *Third*, *economic enticement* is the payment or the satisfaction of basic needs like food or shelter or more complex needs like loyalty and protection. *Fourth*, *transnational*

*recruitment* is described as the coercion of children to act as foreign fighters. *Fifth*, the *compromised basic education sector* refers to the exposure of children through schools in terrorist-controlled regions. *Sixth*, *dissemination of propaganda* refers to exposure to any content that triggers anger or empathy and illicitly aims to recruit children. Last, *online recruitment* refers to any activity of recruiting children using any online tools or means, including but not limited to grooming and targeted advertising.

Both UNSOM (2017: 14) and UNODC (2017: 11 - 13) share overlapping recruitment strategies, such as direct or forced recruitment, third-party recruiting, and recruiting through media or propaganda. Of the latter mentioned 'online recruitment' strategies employed by terrorists and violent extremists, the two (2) strategies used on children include *grooming* perpetrator gradually builds trust with target (online) and *targeted advertising* identifying online behaviour (signifying those vulnerable to advertising with embedded propaganda).

However, UNODC (2017: 22 - 25) argues that challenges remain that prevent a complete prohibition of child recruitment – despite states' alignment to international standards and practices, like international child protection frameworks such as the Convention on the Rights of the Child), or more broadly, universal frameworks against terrorism, such as the resolutions of the Security Council. Furthermore, critical challenges to preventing the widespread recruitment of children include social and cultural norms consideration of children as adults), or shifting the perception of blame because it is a voluntary choice from which the child bears the responsibility, not the recruiter). As a result, the UNODC (2017: 27 - 28) recommended guidance to international frameworks aimed at prohibiting the recruitment of children, including:

(i) Eliminating the prior limitations related to the age of individual recruitment, and suggests raising the legal recruitment age to 18 years;

(ii) Eliminating the distinction between forced recruitment or consensual recruitment of a child, and that this distinction should be taken as legally irrelevant, given the overarching extensions of universal prohibitions of child recruitment;

(iii) recognizing that children may play many other roles in conflict, apart from front-line fighters, including the exploitation of the child in supporting roles; and,

(iv) Prohibiting recruitment of children by any group, whether considered as terrorist, violent extremist, armed groups, non-state groups, or other criminal groups, should be treated the same as when viewed through the lens of the criminalization of child recruitment in terms of international law.

In conclusion, terrorists use the internet and social media to fulfil a broad range of nefarious purposes. A recurring reason across much-referenced material is that terrorists use social media to support recruiting efforts, communications, and operations. A concerning pattern is that many of the illicit recruiting techniques are applied to recruit children online, like grooming or viewing propaganda, potentially via social media. The following is a summarised list of how terrorists use the internet and social media for nefarious reasons, as per the above:

(i) Hossain (2015: 5 - 7): 'operational communication, intelligence gathering, information sharing, recruitment and training';

(ii) Ucko (2018: 255): the internet and social media have been used by Al-Qaeda and ISIS for the radicalisation of sympathizers, draw foreign fighters, and incite further attacks;

(iii) Chigudu (2021: 415): dissemination of extremist content on social media for indoctrination and radicalisation;

(iv) Klausen (2015: 17): Twitter is used for recruitment and indoctrination;

(v) IGAD SSP (2016: 30): operations and communications via the internet;

(vi) UNSOM (2017: 12): recruitment and messaging of Al-Shabaab targeted vulnerable youth aged 10-15 years. UNSOM (2017: 14): Al-Shabaab relies on social media and radio for communications and propaganda dissemination. Additionally, UNSOM (2017: 14) recruitment strategies include direct recruitment, forced recruitment, third-party recruiting, media publicity, religious persuasion; and

(vii) Cox *et al.* (2018: 2): Al-Shabaab used social media for illicit activities, including propaganda dissemination, recruitment, and operations, engaging with active users of YouTube and X formerly 'Twitter'.

## What are Private Companies doing to Reduce Terrorist Content on their Platforms?

There has been much engagement from Western private companies to reduce and limit the spread of terrorist content online and on social media. As owners of the most popular social media platforms, they are deeply invested in content curation, oversight, and other tasks to combat terrorism. They are also accountable for preventing law violations, whether local or international, in terms of terrorism.

In a 2011 hearing before the US Subcommittee on Counterterrorism and Intelligence[13], testimony on terrorism and social media revealed that while radicalisation and recruitment occurred, the number of those who become radicalised from terrorist content in the United States was relatively few. A naval analyst stated that 'if the internet did play a role in radicalisation, it is happening elsewhere', reasoning that 'if you post al-Qaeda propaganda to all of the mainstream websites, only.00001 per cent of the people who viewed it will go out to fight for al-Qaeda and even fewer would carry out suicide operations'. According to Klausen (2016: 45-46), Twitter responded in 2015 to public outcry to exercise greater control on extremist accounts. However, it was not effective, as terrorist recruiters could also resort to the concealment of recruitment posts by communicating in especially those in languages other than English, including Arabic, Urdu and Russian.

In a 2018 hearing before the US Committee of Science, Transport and Communication[14] , a high-ranking Facebook official indicated that 99% of ISIS and Al Qaeda terror content uploaded to Facebook is blocked, explaining that 'this is done primarily through the use of automated systems like photo and video matching and text-based machine learning'. During the same hearing, a high-ranking Twitter official stated that 'while there is no 'magic algorithm' for identifying terrorist content, we have improved the effectiveness of our in-house proprietary technology' and stated that 'our technology supplements user reports, human review, and it significantly augments our ability to identify and

---

[13] *Jihadist Use of Social Media - How to Prevent Terrorism and Preserve Innovation* (2011) 1st session. https://www.govinfo.gov/content/pkg/CHRG-112hhrg74647/html/CHRG-112hhrg74647.htm

[14] *Terrorism and Social Media:#Isbigtechdoingenough?* (2018) 2nd session. https://www.govinfo.gov/content/pkg/CHRG-115shrg31316/html/CHRG-115shrg31316.htm

remove bad content from Twitter'.

According to Macdonald *et al.* (2019: 183), Facebook, Twitter, and YouTube's terms of service ToS) have strong mandates to disrupt terrorist content on their platforms. However, Macdonald et al. (2019: 194) found a danger in ToS due to a discrepancy between 'the offence definition and the wrong that was being targeted'. Two years prior, in 2017, Meta explained how they had planned to use artificial intelligence AI) to automatically identify and reduce terrorist content across apps and services on their platform, which included the following AI detection methods, including *image matching*, *language understanding*, *removing terrorist clusters*, *reducing recidivism*, and *cross-platform collaboration*. First, *image matching* refers to comparing newly uploaded images to known offensive images, and if an image matches known prior offensive content, then it is blocked and will remain blocked from all further attempts to publish online. Second, *language understanding* refers to models trained to look for offending text that violates usage terms. Third, *removing terrorist clusters* refers to models that detect connections between offending profiles to identify networks of illicit activity. Fourth, *reducing recidivism* means preventing offending users from repeatedly creating new accounts, thereby dodging access bans. Fifth, *cross-platform collaboration* refers to active counter-terrorism re-tooling applied across products and services owned by Meta, such as WhatsApp and Instagram, to detect illicit content.

In 2016, an open-source method dedicated to combatting terrorist online content, known as 'The Redirect Method', was created by private start-up company Moonshot. The Redirect Project self-describes its internal operation as 'just as other companies use ads on social media and search engines to sell material products to an audience defined by, in whole or in part, the keywords they are searching for, the Redirect Method places ads in the search results and social media feeds of users who are searching for pre-identified terms that we have associated with a particular online harm'. Furthermore, they states that 'the Redirect Method shows those users content which responds to and counters socially harmful narratives, arguments and beliefs espoused by the content for which they were originally searching'. According to Helmus and Klein (2018: 7) and the UNODC (2017: 33), the Redirect Method was co-created by a subsidiary of Google, and its underlying operation works by displaying advertisements that link back to YouTube video playlists available in English and Arabic that covertly aim to counter ISIL propaganda when any of a specific, pre-determined set of ISIL related keywords are entered into a Google search.

Helmus and Klein (2018: 11), who completed a case study of the Redirect Method titled '*Assessing Outcomes of Online Violent Extremism*' CVE), found that while impact evaluations are complicated, the Redirect Method was successful in 'effectively exposing individuals searching for violent jihadist or violent far-right content to content that offered alternative narratives', and that 'users clicked on these ads at a rate on par with industry standards'.

Furthermore, Meta (2016) demonstrated a willingness to collaborate on developing new technologies to reduce illicit content on their platforms, including the companies of Facebook, X formerly 'Twitter'), YouTube and Microsoft, who announced the creation of their industry-wide database of digital fingerprints of offending digital content. The form of information in the database is file hashes of illicit content produced by or in support of terrorist organisations in 2016. The hashing method is effective because every file has a corresponding hashed value that can accurately identify the file on a system. If two hashes match, then it is certain that the content in question is offensive or illicit. According to Meta (2016), the technology enables each company to block content relating to terrorist activity across their platforms using the hash values that represent or identify a file; thereby, the ability of terrorists to jump from one platform to another to spread illicit content is reduced. Depending on updates and maintenance, such tools may solve the problem of the top-down architecture of illicit content reposting or redundancy, as described by. It is important to note that states are free to legislate on their own accord and take other steps, such as designing similar tools, such as the one mentioned above.

In January 2022, Meta stated that it became the chair of the cross-industry counter-terrorism organisation called '*The Global Internet Forum to Counter Terrorism*' GIFCT. The GIFCT (2023) stated that it 'brings together the technology industry, government, civil society, and academia to foster collaboration and information-sharing to counter terrorist and violent extremist activity online'. In late 2022, Meta's President of Global Affairs stated that they would make their hash technology publicly available as an open-source content moderation tool called 'Hasher Matcher Actioner'. Meta (2023) reported that it took action on over 16 million items of 'dangerous organisations' content' between January and March 2022 and 16.7 million from July to September 2022. Databases of offending terrorist content hashes, such as that by the GIFCT, can be used to complement and enhance the databases of international organisations, such as INTERPOL's nineteen (19) criminal databases, to assist in the criminalisation of terrorism.

The open sourcing of the Hasher Matcher tool and efforts of other pri-

vate companies like X formerly 'Twitter'), YouTube, Microsoft and Moonshot show that private social media companies are committed to a transparent and collaborative approach to eliminating terrorist content online. Furthermore, Meta's Hasher Matcher database of offending terrorist content hashes can be used to complement and enhance the databases of international organisations, such as INTERPOL's nineteen (19) criminal databases, which include databases and sub-databases of data on individuals, forensics, travel and official documents, stolen property, firearms tracking, and organised crime networks. In combination, open-source tools and pre-existing tools can be combined to assist in the criminalisation of terrorism.

In conclusion, private companies have taken steps toward reducing terrorist content online and on their platforms. The review does not focus on the efficacy of such systems. This warrants consideration because technology is often proprietary. However, there is some cooperation and shared understanding between the companies about certain aspects, like the need to block offensive content, which should be removed as soon as reasonably possible. The review now summarises some of the ways that private companies sought to reduce terrorist content on their platforms, not limited to:

(i) The use of terms of service ToS) agreements Macdonald *et al.* (2019: 183);

(ii) Automatic identification and removal of offending content, including *image matching, language understanding, removing terrorist clusters, reducing recidivism, and cross-platform collaboration*;

(iii) Open-source projects, like The Redirect Method by Moonshot, can redirect some vulnerable users to counter-narratives through targeted advertising; and,

(iv) Broader collaboration and agreement between social media companies to reduce terrorist content.

## *Q4: Case Study: How do Broad Bans on Terrorist Content on Social Media Impact Journalists and Civil Society?*

This case focuses on Somalia, a country in East Africa. There are many instances of violence, attacks, deaths, and bombings reported in the media, but

also that the situation is changing and dynamic. Generally, the selection of case material considered the availability of data: a non-BRICS member, a developing country on the African continent, where there is a government and military, but there are violent extremism problems – the researcher chose the Federal Republic of Somalia from this pool. The case hinged on the recency, accessibility, and quality of reporting made available by all responsible parties included or mentioned in this research. The case begins by investigating the background and history of illicit actors. Therefore, this research question is broken down into three (3) smaller chunks, including:

(i) Background – Al-Shabaab;
(ii) Background – Counterterrorism: Developments of policy, state, and military activity in Somalia; and
(iii) Case study: How do broad bans of terrorist content on social media impact journalists and civil society?

## Background – Al-Shabaab

Al-Shabaab, the East African affiliate of Al-Qaeda, has executed many deadly attacks across Somalia, as will be described. Anzalone (2020: 30) states that Al-Shabaab has proven to be 'markedly resilient in the face of numerically, economically, and technologically superior enemies, including the Somali Federal Government SFG) and its main international supporters, the United Nations, United States, European Union, and African Union AU) Mission in Somalia AMISOM) forces'. Furthermore, their research describes the self-promotion tactics of Al-Shabaab, such as making documentary-style films, and describes prior events involving the Al-Shabaab group, notably their interest in engaging with people through the creation of propaganda:

> It continues to retain significant, deadly military capabilities and the ability to plan and successfully execute mass-casualty attacks in the heart of Somali cities, including the federal capital, Mogadishu, and on government military bases. The Somali militant group, which regularly engages in anti-civilian violence both in its terrorist attacks and as a tool of the proto-state governance of areas under its control, also continues to run a highly capable media operations apparatus that produces glossy propaganda material aimed, often in the same media product, at domestic Somali, regional East African, and international audiences.

According to AmaniAfrica (2022), in November 2022, Al-Shabaab executed two deadly bombings in Mogadishu as recently as 29 October 2022, wherein more than 120 lives were lost, and hundreds of others received critical medical care. Furthermore, Al-Shabaab fighters carried out another bombing on a Somali military base in the Galgaduud region just mere days later, wherein the base defenders suffered casualties, and the attackers looted small arms and vehicles. The following year, AmaniAfrica (2023) published a follow-up report stating that 'the possibility of Al-Shabaab acquiring commercial drones to enhance its capabilities seems also to have become a major concern' remains.

On 4 January 2023, two car bombs killed fifteen in the Hiraan region of Somalia. On 22 January 2023, international news agencies reported that Al-Shabaab fighters attacked the Office of the Mayor in the capital, Mogadishu, with security forces later regaining control of the situation that left several attackers, defenders and civilians dead. A correspondent for a local online news outlet stated a day later that:

> Two car bombs detonated by Al-Shabaab militants in central Somalia on Wednesday killed at least 35 people, including eight members of a single family, and wounded 40 more, a senior police officer said. The attack in the town of Mahas was the latest in a series by al Qaeda affiliate al-Shabaab since government forces and allied clan militias last year began pushing the insurgents out of territory they had long held. 'Most of the dead are civilians. They are women and children', said the deputy police commissioner of Hirshabelle State. 'Only one child survived from a family of nine members. Other families also lost half of their members. The two suicide car bombs burnt many civilian homes to ashes'.

Of the cases described above, approximately 170 lives have been lost, and over 50 are injured period: 2020-2023. In reality, many more attacks have taken place, and countless lives have been lost or impacted. In conclusion, the following is a summarised description of the illicit activities of Al-Shabaab, based on all of the above:

(i) The association is experienced, resilient, and self-promotes through propaganda

(ii) Opposed by the Somali Government, the UN, the US, EU and AU;

(iii) Conflict in towns and cities: Mogadishu, Galguduud, Mahas;

(iv) Offensive attacks and bombings target key locations like civilian spaces, governmental offices, and military assets; and,

(v) Concern for the use of drone technology.

With utmost respect to human life lost and all those harmed by hatred, as well as the Government and people of Somalia, the situation has seen improvements, including steady gains in national security and capacity building. State and national security developments warrant further investigation, as described below.

## Background – Counterterrorism: Developments of Policy, State, and the Military in Somalia

Jain and Vaidya (2020: 2) state that 'social media can be of a great help for military, defence and public concerning safety during an unfortunate terrorist event'. The benefits of social media for public safety and, more broadly, for gathering information and combatting terrorism online cannot be ignored. However, it is also essential to understand how the Federal Republic of Somalia has made strides in their policy, state, and military mandates toward effectively combatting such social problems. Therefore, the following investigates successful policy, government, and military developments in the Federal Republic of Somalia.

According to a UNSC press release, in March 2022, the Security Council unanimously adopted Resolution 2628[15] UNSC 2022b. According to Resolution 2628, wherein the AU Peace and Security Council endorsed '*The African Union Mission in Somalia*' AMISOM) into a new entity called '*The African Union Transition Mission in Somalia*' ATMIS), whose mission is to reduce the threat posed by Al-Shabaab, support regional capacity building in terms of the integration of the Somali security and police, conduct a measured handover of security responsibilities to the Government, and, to support the country and region in attaining peace and security.

[15] See Resolution 2628, Article 22. Available at: https://undocs.org/en/S/RES/2628 (2022)

On 1 April 2022, ATMIS assumed the role of AMISOM. ATMIS is a 'multidimensional mission, including military, police and civilians, that is authorised by the African Union and mandated by the United Nations Security Council, under the AU Peace and Security Council'.

According to the *Communique of the 1112th Peace and Security Council*[16] PSC) meeting held on 10 October 2022, derived from '*The Report of the Chairperson of the Commission on the Situation in Somalia and the Mandate of ATMIS*', the PSC wrote the following regarding situational awareness of terrorism on social media:

(i) Article 2: Welcomed the Somali Transition Plan (STP);

(ii) Article 3: Condemned Al-Shabaab as responsible for an attack on 3 October 2022 on the Lamagalaay Somali Military Base Camp in Beledweyne town;

(iii) Article 4: Reiterated the unwavering commitment of the AU through ATMIS in its continued support of the Federal Government of Somalia;

(iv) Article 5: Noted concern for a delayed implementation of the STP and National Security Infrastructure (NSA);

(v) Article 6: Called for a drawdown of troops by 31 December 2022, the handover of Forward Operating Bases FOBs), and called the further implementation of the STP by the handover of security responsibilities from ATMIS to the Somali Security Forces, in line with UN Security Council Resolution 2628 mentioned above), and its developments;

(vi) Article 11: Expressed a deep concern about the upward trend of disinformation campaigns that target ATMIS on social media and urged the authorities to take the necessary steps to prevent and address the issue of incitement of hatred and hold accountable those responsible for such incitement and,

[16] Communication. *Communique of the 1112th Peace and Security Council.* See Art. 6. Available at: https://www.peaceau.org/uploads/eng-communique-for-the-1112th-psc-meeting.pdf

(vii) Articles 12 and 13: Gave tribute to the SSF, ATMIS troops, police and other personnel who have displayed unwavering commitment toward peace in Somalia.

According to AmaniAfrica (2022), interventions by the AU through ATMIS, and with cooperation and support from the Somali Security Forces SSF), have led to many successful operations and outcomes in Somalia. On 21 January 2023, the Maslah Forward Operating Base FOB), a critical security infrastructure, was formally transferred to the Federal Government of Somalia by ATMIS. According to ATMIS 2023a), The Maslah FOB under the control of the Government of Somalia will strengthen security in the region because 'it enables troops to secure the major supply route connecting Mogadishu and the hinterland hence ensuring the safe and secure movement of goods and services, which is important for both economic and social development of this country'. This event signifies a transfer of strength and security that will significantly benefit the government and people of Somalia and the success of other humanitarian projects in the region aimed at building capacity.

As per '*The Comprehensive International Framework to Counter Terrorist Narratives*'[17], wherein Article 19 states, 'it is argued, also to offer alternative or positive narratives, especially when terrorists seek to exploit genuine grievances; effective narratives must take into account genuine feelings of powerlessness and alienation and provide credible alternatives, especially to vulnerable young people searching for a sense of meaning in their lives'.

According to the Centre for International Media Assistance CIMA, (2007) report titled '*Community radio: its impact and challenges to its development*', 'like a vaccine capable of reducing preventable diseases, community radio is a simple, effective solution to achieve development goals, to prevent fragile states from becoming failed states, and also to help people celebrate their own culture'.

In September 2020, under the auspice of the UN's Food and Agriculture Organisation FAO), a capacity-building initiative was created and launched across eight local radio stations inside Somalia. The online press release and the UN news story are matching sources, which explain that due to relatively lower levels of literacy in rural areas of Somalia, the medium of radio enables individuals involved in the agricultural and primary production sectors to access the news and information. Furthermore, the initiative targeted farmers through

[17] per *S/2017/375,* mentioned earlier. See footnote 9.

the medium of radio, which increased accessibility and inclusiveness, explaining that 'using an interactive and participatory communication tool such as radio ensures that no one is left behind and progress is made towards achieving the sustainable development goals'. According to the FAO (2022), the pilot project period was 2020/2021 and featured 58 episodes, which was later expanded in 2021/2022 and increased the total number of episodes to 110. The above is a short investigation of open sources about successful policies, government, and military developments aimed at combating terrorism and countering terrorist narratives in Somalia. The focus is on open sources like UNSC resolutions, press releases, communiques, news reports, and published materials of military organisations, states, and NGOs.

## Case Study: How do Broad Bans of Terrorist Content on Social Media Impact Journalists and Civil Society?

Here, the investigation focuses on how broad bans on terrorist content can impact journalists and civil society through a case study of a Somali journalist. This part of the review focuses on contextualising the events leading up to and after the journalist was arrested. There are many specific ways in which the broad bans on illicit terrorist content on social media affected their life – this is highlighted by a summary, which later concludes the section.

On 8 October 2022, the Ministry of Information, Culture and Tourism of Somalia MIS) broadly banned terrorist content on social media, published as a press release on their verified Facebook page and further disseminated by the verified Twitter account of the Somali National News Agency. The press release states that 'the public was warned to avoid spreading terrorists' intimidating and misleading messages – whether intentionally or unintentionally, directly or indirectly and consciously or unconsciously'. Furthermore, the 8 October 2022 press release above aptly stated that 'the Federal Govern-ment of Somalia considers as a crime the act of disseminating the messages of the terrorists, [and], any media or an individual that promotes and encourages the acts of the brutality of the terrorists will face the law, and actions will be taken if they are found guilty of violating the proper use of the media/social media'. Lastly, the press release also called for the Protection of freedom of expression, giving a final call that asked every citizen to report suspicious social media accounts.

On 12 October 2022, the Ministry of Information, Culture and Tourism of Somalia published a follow-up press release on their verified Facebook and

X formerly 'Twitter') accounts, commenting on the arrest of Mr Mumin. A. A. and acknowledging that he is in the custody of the authorities, owing to security-related charges, and not for, or related to his work as a journalist. What is important is that after he has been arrested, he will struggle to continue reporting on their desired subject matter in future, due to the broad bans of terrorist content. A tweet from the Official British Embassy Mogadishu, @UKinSomalia, which attached a picture of Mr Mumin in a blue suit, and expressed their deep concern for the arrest and detention of @Cabdalleaxmed, urging due process and fairness in the hearing of his case.

In a later Facebook post on 18 January 2023, the Ministry of Information of Somalia stated that in its mission to eradicate terrorism, the Federal Government employed a three-pronged strategy comprising a military offensive, curbing illicit finance and funding of terrorist organisations, and implementation of an ideological strategy in which the media plays a role. Furthermore, the post stated that in the future, the duties of the Government Communication Office will include creating communications and media plans, growing social media presence, including crisis communications and communications in the private sector, and lastly, monitoring and evaluating the implementation of projects within its scope.

Carthy and Sarma (2021: 2 - 3) explained that a counter-narrative must provide a new way to see narrative-related propaganda and that, when done correctly, it transforms how a real-world event may be perceived. The journalist in question, Mr. Mumin, has written for The Guardian on topics contributing to the dissemination of counter-terror narratives, which align with the UNGTS' four pillars to combat terrorism, as mentioned earlier:

(i) reporting on terrorist attacks in Somalia, such as bombings, and accounts of survivors;
(ii) citizens fear Al-Shabaab retribution for owning cell phones, internet access, and music – types of media outlawed by Al-Shabaab;
(iii) social recreation and celebration despite fear;
(iv) war in Yemen;
(v) extreme climate conditions and famine in Somalia; and
(vi) challenges faced by Somali people during the Covid-19 pandemic;

On 12 December 2022, Human Rights Watch published a joint letter, co-signed by many Non-Governmental Organisations NGOs) and news agencies, which

called for the easing of restrictions on Mr Mumin. A.A., among all other journalists:

(i) Amnesty International;
(ii) ARTICLE 19 Eastern Africa;
(iii) Committee to Protect Journalists;
(iv) Human Rights Watch;
(v) International Press Institute IPI);
(vi) PEN International; and,
(vii) Robert F. Kennedy Human Rights
.

The letter was addressed to the Attorney General of the Federal Republic of Somalia and asked to 'end all threats, harassment, intimidation, and arbitrary arrests and detention of journalists and civil society actors' and additionally asked the Office of the Attorney General to cease all charges against Mr Mumin. A. A., who holds the position of Secretary General of the Somali Journalists Syndicate. Furthermore, the HRW 2022a) letter states that 'Mumin's arrest came a day after he, along with directors of four other media organisations, raised concerns that, on 8 October [2022], a directive from Somalia's Ministry of Information that prohibited the dissemination of extremism ideology messages, both from traditional media broadcasts and social media, could restrict legitimate free speech'.

Furthermore, much evidence points to increased threats to journalism activities in this case. According to the Reporters Without Borders annual press freedom index, Somalia has ranked 163, 161, and 140 out of 180 countries for 2020, 2021, and 2022 respectively. By comparison, BRICS countries scored the following averages across the years 2020, 2021 and 2022:

(i) Brazil: 109;
(ii) Russia: 151;
(iii) India: 145;
(iv) China: 176; and,
(v) South Africa: 33.

According to the Somali Mechanism for Safety of Journalists annual report titled '*Journalists Safety and Media Freedom in Somalia*' (SMSJ 2021), 53, 56, and 66 journalists were arrested in 2019, 2020, and 2021, respectively, and there were 39 incidents of physical assaults, attacks, intimidation and threats against

journalists in 2021. In 2021, 44% or almost half of the attacks against the media and journalists were reprisals for unfavourable reporting, and 5% were due to critical social media posts. The report alleged that some officials adopted a culture of 'enforced secrecy', which aimed to stifle criticism and silence knowledge of corruption. Anzalone (2020: 31) attributed a lack of official transparency and clear communication allowed for the dissemination of Al-Shabaabs' narratives in this case.

As a result of the lack of access to official sources of information, journalists working in Somalia came to depend on unreliable sources from social media regarding user-generated content and political leaks. Furthermore, stating that 'fake news' permeated social media during the Covid-19 pandemic, and described the situation as:

> The lapse in collaboration empowered peddlers of fake news on social media and allowed online rumours and misinformation to go unchallenged, probably contributing towards low COVID-19 vaccine uptake. Some online fake news found its way into traditional media and was readily amplified by unsuspecting journalists without access to official facts and data.

There are many reasons why journalists and civil society can enter the crossfire of bans on terrorist content on social media. The 2019 *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while countering terrorism*[18] states that between the years 2001 and 2018, 'at least 140 Governments had adopted counter-terrorism legislation', but '66 per cent of communications sent by holders of the mandate between 2005 and 2018 concerned counter-terrorism measures directed at civil society actors or human rights defenders'. The report recommended that 'civil society and human rights experts must be meaningfully and consistently given access to the United Nations counter-terrorism architecture'. For these and other forthcoming reasons, journalists and civil society are vulnerable in such circumstances.

Klausen (2016) states that 'it is important to suppress internet producers – not consumers – of online violent extremist content'. Furthermore, Klausen

[18] Report. *A/74/335.* Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism Available at: https://undocs.org/A/74/335

(2016) explains some of the main issues with broad bans on terrorist content on social media, likening it to indiscriminate suppression of information, noting the loss to law enforcement:

> A policy of indiscriminate suppression of terrorist communication on frontline open social media platforms is comparable to disconnecting the fire alarms all over the house. It deprives law enforcement of important tools for tracking domestic terrorist networks by forcing online extremists to migrate to domains and service providers that exercise less control over content or no control at all. Removing online content containing direct threats or that violates the rights of victims and their families should remain a high priority. Pushing online extremism onto encrypted sites will also make it more difficult for parents, authorities, and concerned bystanders to detect early signs of radicalisation. Moreover, it makes it impossible to deliver targeted online counter-messaging to population groups considered to be vulnerable to terrorist recruiters.

Furthermore, the broad bans on terrorist content may have indirectly placed journalists at risk of violent retribution from terrorists in Somalia for complying with content restrictions. In their press release, the Somalia Media Fraternity SMF) expressed concerns about the directive on 8 October 2022 released by the Ministry, which created a broad ban on posting terrorist content or messages. They stated that 'the new directive already brought security concerns for some local journalists and media houses after a counter-directive was issued by al-Shabaab threatening journalists and other entities that implement the government directive'.

In a statement, Mr Mumin, A. A. said that 'the government was putting lives at risk as al-Shabaab had threatened to kill any journalists who followed the new directive'. The implication is that lawfully complying with bans may lead to journalists becoming the target of retribution from extremists or terrorists. According to the SABC news subsidiary, Channel Africa (2022) news report, Al-Shabaab claimed that the Somali government entered a 'campaign to silence the truth', warning internet service providers in the region to avoid the blocking of its web traffic.

The above case material shows that Al-Shabaab cares about its public presence and will ensure its imaging is continually conveyed through the media and the internet. The following summarises some of the ways that broad bans

on terrorist content on social media have impacted the lives of journalists and civil society, as mentioned above:

(i) Unclear instructions and legal implications: the press release MIS (2022b); SONNA (2022) states that 'the public was warned to avoid spreading terrorists' intimidating and misleading messages – whether intentionally or unintentionally, directly or indirectly and consciously or unconsciously';

(ii) Conflict with official counter-terrorism narratives and strategic objectives;

(iii) Journalists unable to work;

(iv) Complying with bans means that fake news, online rumours and misinformation become perpetuated;

(v) Complying with bans does not support the creation of positive narratives, in line with the UNGA (2006b: 4 - 9);

(vi) If journalists choose to comply with bans lawfully, they can experience threats or intimidation from extremist or terrorist groups;

(vii) If journalists do not comply with bans, they can face punishment like intimidation, threats, detention, or legal action from the Government; and,

(viii) While extremist content should be removed immediately, over-policing of digital spaces pushes extremism onto encrypted technologies, making it harder for parents to monitor the activities of children.

# 4 Findings

## *4.1 Summary: What are the Policy Mechanisms of the UN that Members Use to Engage in Counterterrorism and Combatting Terrorist Narratives?*

According to the research, members of the UN engage in counter-terrorism through the mechanisms of UNGA frameworks, including the UNSC, and other

activities and initiatives. First, members engage through the UN Security Council framework by aligning with the UNGCTS resolution *A/RES/60/288*, its review updates, and supporting the UNGA and Security Council's resolutions and decisions about its implementation.

In 2015, the UNGA adopted *Agenda A/70/674*, titled '*The Plan of Action to Prevent Violent Extremism*'. This Plan established a three-point system that covered a broad spectrum of methods to combat violent extremism as conducive to terrorism and to create the necessary rule of law initiatives.

Third, members may counter terrorist narratives online, according to the '*Comprehensive International Framework to Counter Terrorist Narratives*'[19], per resolution *S/2017/375*. This framework states that countering terrorist narratives comprises three core elements: 'legal and law enforcement measures per obligations under international law and consistent with United Nations resolutions; public-private partnerships; and counter-narratives'.

Fourth, states engage with the UN subsidiary bodies, committees, monitoring teams, and working groups, supporting the broader UN's counter-terrorism efforts and sustainability goals. Members engage in counter-terrorism through mutual engagement with subsidiary bodies of the UNSC, including committees like:

(i) the Counter-Terrorism Committee CTC);
(ii) the Counter-Terrorism Executive Directorate CTED);
(iii) the UNOCT;
(iv) the UN Counter-Terrorism Centre UNCCT); and,
(v) working groups that aim to support coordinating efforts to combat terrorism at all levels.

Additionally, a repository of relevant legal instruments, is publicly available OHCHR (2023a; 2023b).

The repository includes in conventions, protocols, treaties, resolutions, and regional instruments, penned by the Special Rapporteur on Counter-Terrorism and Human Rights, titled 'International Standards on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism', and, all annual publishing's of the Special Rapporteur to the Human Rights Council HRC) and UNGA,

[19] Per S/2017/375, mentioned earlier. See footnote 9.

## *4.2 Summary: What is the BRICS Approach to Combatting Terrorism on Social Media through the Lens of the last five (5) Summit Declarations?*

Over the last five (5) years, from the 10th to the 14th BRICS Summits from 2018 to 2022, BRICS Declarations have become increasingly connected with the themes of terrorism, the internet, and the recognition of social media. At the 2018 Johannesburg Summit Declaration, members committed to future strategic cooperation and addressing opportunities and challenges posed by the Fourth Industrial Revolution.

In the 2019 Brasilia Summit Declaration, members reaffirmed their commitment to condemn terrorism and engage in multilateral efforts to reduce it.

In 2020, the 12th BRICS summit was convened virtually in Moscow, Russia. The summit's theme was '*BRICS Partnership for Global Stability, Shared Security, and Innovative Growth*'. The summit's conclusion saw the adoption of The Moscow Declaration and the BRICS Counter-Terrorism Strategy.

The BRICS (2020b: 5) Counter-Terrorism Strategy represents the first recognition of the themes of terrorism, the Internet and social media: 'to counter extremist narratives conducive to terrorism and the misuse of the Internet and social media for terrorist recruitment, radicalisation and incitement and providing financial and material support for terrorists'.

In 2021, the 13th BRICS summit was held virtually in New Delhi, India, and concluded with the adopting of *The New Delhi Declaration* and the aligned *BRICS Counter-Terrorism Action Plan* CTAP. In 2022, the 14th BRICS summit was held in Beijing, China, and members reaffirmed their commitment to promoting an open, secure, stable, accessible and peaceful ICT environment.

## *4.3 Summary: Why do Terrorists use Social Media, and what are Private Companies doing to reduce Terrorist Content on their Platforms?*

From the above review, it is clear that terrorists use the internet and social media to fulfil a broad range of nefarious purposes. A recurring reason across much-referenced material is that terrorists use social media to support recruiting efforts, communications, and operations. A concerning problem is that many of the illicit recruiting techniques have the potential to be applied to recruit

children online, like grooming or viewing propaganda, potentially using social media. In conclusion, the following list summarises how terrorists use the internet and social media for nefarious reasons, as per the reviewed data found earlier in this section:

(i) Hossain (2015: 5 - 7): 'Operational communication, intelligence gathering, information sharing, recruitment and training';

(ii) Ucko (2018: 255): the internet and social media have been used by Al-Qaeda and ISIS for the radicalisation of sympathizers, draw foreign fighters, and incite further attacks;

(iii) Chigudu (2021: 415): dissemination of extremist content on social media for indoctrination and radicalisation;

(iv) Klausen (2015: 17): Twitter is used for recruitment and indoctrination;

(v) IGAD SSP (2016: 30): operations and communications via the Internet;

(vi) UNSOM (2017: 12): recruitment and messaging of Al-Shabaab targeted vulnerable youth aged 10-15 years. UNSOM (2017: 14): Al-Shabaab relies on social media and radio for communications and propaganda dissemination. UNSOM (2017: 14): Specific recruitment strategies include direct recruitment, forced recruitment, third-party recruiting, media publicity, religious persuasion, and

(vii) Cox *et al.* (2018: 2): Al-Shabaab used social media for illicit activities, including propaganda dissemination, recruitment, and operations, engaging with active users of YouTube and X formerly 'Twitter'.

In conclusion, private companies are making some rightful steps toward reducing terrorist content online and on their platforms. The review does not analyse whether the responsibility can be entirely entrusted to international companies operating inside multiple jurisdictions.

However, it should be acknowledged that some Western companies have cooperated toward a shared understanding of terrorist content and that such content should be removed as soon as reasonably possible. The review shows

some ways that private companies have acted to reduce terrorist content on their platforms, summarised as:

(i) The use of terms of service (ToS) agreements Macdonald *et al.* (2019: 183);

(ii) Automatic identification and removal of offending content, including *image matching, language understanding; removing terrorist clusters, reducing recidivism, and cross-platform collaboration*;

(iii) Open-source projects, like The Redirect Method by Moonshot, can redirect some vulnerable users to counter-narratives through targeted advertising;

(iv) Broader collaboration and agreement between social media companies to reduce terrorist content.

## 4.4 Summary: Case Study: How do Broad Bans on Terrorist Content on Social Media impact Journalists and Civil Society?

As a result of heightened tensions between the Government, journalists, and terrorist groups in Somalia, the research brought to light how broadly banning terrorist content on social media can impact independent journalism and civil society. The research drew on a case study with unique implications regarding banning illicit content on social media.

Noting that the journalist was not directly charged for their work as a journalist, the broad bans on terrorist content affected his ability to operate within his professional capacity after that. With respect, the case of a Somali press release illustrated an instance of policies to ban terrorist content to the detriment of press media and civil society, neither of which may necessarily have the intention to incite further terrorist acts when sharing or transforming terrorist content on social media.

The following summarises some of the ways that broad bans on terrorist content on social media have impacted the lives of journalists and civil society, drawing from a case of a Somali journalist:

(i) Unclear instructions and legal implications: the press release MIS (2022b); SONNA (2022) states that 'the public was warned to avoid spreading terrorists' intimidating and misleading messages – whether intentionally or unintentionally, directly or indirectly and consciously or unconsciously';

(ii) Conflict with official counter-terrorism narratives and strategic objectives;

(iii) Journalists unable to work;

(iv) Complying with bans means that fake news, online rumours and misinformation become perpetuated;

(v) Complying with bans does not support the creation of positive narratives, in line with the UNGA (2006b: 4-9);

(vi) If journalists choose to comply with bans lawfully, they can experience threats or intimidation from extremist or terrorist groups;

(vii) If journalists do not comply with bans, they can face punishment like intimidation, threats, detention, or legal action from the Government; and,

(viii) While extremist content should be removed immediately, over-policing of digital spaces pushes extremism onto encrypted technologies, making it harder for parents to monitor the activities of children.

## 5 Discussion

In their research, UNSOM (2017) asked respondents to consider what particular role they might play in combatting youth recruitment into Al-Shabaab as influential members of their society. A respondent among the parents, teachers and civil society group in Mogadishu said:

> I can use social media by posting about the ills of Al-Shabaab and posting good information about the country, like how the country is progressing in various sectors such as agriculture, education, and

> health, so that youth can feel the goodness and the purpose of having a Somali government.

Furthermore, a female youth respondent from Mogadishu said:

> I can use YouTube and Facebook to share the evil acts of terrorism and, at the same time, call for Somali unity. This message I will share with all my friends.

Under such restrictions of broad content bans, such as in Somalia, respondents would not be permitted to share their experiences, with the threat of incurring penalties for intentionally or unintentionally violating bans of terrorist content on social media. Similarly, such rules would apply to all journalists like Mr Mumin. This presents implications for BRICS and the broader security community in future discussions around controlling terrorist content on social media. Policymakers must consider that broad content restriction may result in undue or harsh punishment of journalists or civil society – provided that a discernible will to incite further violence is not present.

Recalling the critical moment that occurred on 8 October 2022, wherein the Somali Ministry of Information MIS) published a press release on both their verified Facebook page and in a Tweet by the Somali National News Agency. In this press release, as cited, 'the public was warned to avoid spreading terrorists' intimidating and misleading messages – whether intentionally or unintentionally, directly or indirectly and consciously or unconsciously'.

Furthermore, the release states that 'the Federal Government of Somalia considers as a crime the act of disseminating the messages of the terrorists; meanwhile, any media or an individual that promotes and encourages the acts of the brutality of the terrorists will face the law, and actions will be taken if they are found guilty of violating the proper use of the media/social media'.

Independent media and press reporting conducted without bias, persuasion, or intimidation, including that conducted online on social media, can create organic counter-terror narratives by disseminating information that challenges the dominance of extremist narratives and power structures of terrorist organisations. 'Truth-telling', in the idealistic sense of providing accurate and reliable information via journalistic investigation, is a fundamental aspect of accurate reporting, and it can be a powerful tool for the public creation of counter-narratives.

From a zero-sum perspective, every journalist detained is one less that can report on the fruitful outcomes of regional approaches to counter-terror. Furthermore, they will be unable to create positive content on social media during that time, and the same applies to members of civil society, such as those victims who may wish to share their experiences with the public. This is a loss to regional approaches to counter-terrorism online.

Furthermore, many information transformations would become impossible, as indicated in the above example of female youth respondents in the UNSOM (2017: 15) research, wherein youth respondents wished to contrast 'evil acts of terrorism', and simultaneously 'call for Somali unity'. This is an organic transformation of information, and simultaneously, a decentralised counter-narrative is created. The purpose of a counter-narrative, as described by Carthy and Sarma (2021: 2 - 3), is to provide a new way to see narrative-related propaganda, and when done correctly, it transforms how a real-world event can be perceived.

In these ways, broad content restrictions and the harsh punishment of journalists and civil society actors can be seen as a loss of human resource capacity to generate organic and decentralised counter-terror narratives. Similarly, this outcome includes any limitations on public information sharing.

## 6 Recommendations

- Creating inclusive policy discussions that aim to combat terrorism in all its prior and emergent forms, such as terrorist content and social media, while being mindful of the role of journalists and civil society in their capacity.

Such discussions can occur without the ability of those or other such policies or frameworks to be weaponised against them in the future or to prevent them from doing work or exercising free will in any capacity because journalists or civil society actors do not intend to incite further acts of terror.

- Engaging in open-source, public, and collaborative intelligence gathering, intending to suppress new illicit terrorist content posted by online terror organisations. This could be done by integrating open-source tools and technology developed by private companies – such as Meta's

Hasher Matcher or The Redirect Project – and cooperating with private companies and experts from the international community. Social media companies are in many parts of the world, not just the West.

Such an approach could be regional and top-down, focusing on suppressing the producers of illicit content with discernible intent to incite further violence, such as focusing on members of known groups.

- Ensuring that, when necessary, bans of terrorist content on social media must accompany an awareness to protect further journalists and civil society actors, who may incur threats from terrorist groups as retribution for lawful compliance with official directives, rules or laws. This avoids any '*damned if you do, damned if you do not*' scenarios for journalists and civil society actors.

For example, in response to the ban on the dissemination of terrorist content on 8 October 2022 in Somalia, as issued by the Somali Ministry of Information, Mr A.A. Mumin stated that 'al-Shabaab had threatened to kill any journalists who followed the new directive'.

## References

@UKinSomalia [@UKinSomalia] 2022. 13/10/ October 2022. *The United Kingdom is Deeply Concerned by the Arrest & Detention of @Cabdalleaxmed, Secretary General of @Sjs_Somalia.* [Tweet.] https://twitter.com/UKinSomalia/status/1580596836603432962

Ahmad, A. 2022. *Exploring the Role of Social Media within COVID-19 Prevention and Mis/Information on Facebook: A Case Study of the South African Level 5 Lockdown.* University of KwaZulu-Natal.

Al Jazeera 2023a. *Al-Shabab Claims Deadly Car Bomb Attack in Central Somalia*. Avaialable at: https://www.aljazeera.com/news/2023/1/4/car-bombs-kills-civilians-level-houses-in-central-somalia?traffic_source=KeepReading (Accessed on 17 January 2023.)

Al Jazeera 2023b. *At Least Five Killed in Bomb, Gun Attack in Mogadishu*. Available at: https://www.aljazeera.com/news/2023/1/22/several-injured-after-blast-at-mayors-office-in-mogadishu (Accessed on 17 January 2023.)

AmaniAfrica. 2022. *Situation in Somalia and Operations of Atmis*. Available at: https://amaniafrica-et.org/situation-in-somalia-and-operations-of-atmis/ (Accessed on 12 January 2023.)

AmaniAfrica. 2023. *Situation in Somalia and Operations of Atmis*. Available at: https://amaniafrica-et.org/briefing-on-the-situation-in-somalia-and-the-phased-drawdown-of-atmis/ Retrieved 22/03/2023 from

AMISOM. 2022. *Amisom - Frontpage*. https://amisom-au.org

Amnesty International 2022. Somalia: Authorities Must Immediately and Unconditionally Release Journalist Abdalle Ahmed Mumin. https://www.amnesty.org/en/latest/news/2022/10/somalia-authorities-must-immediately (Accessed on 18 January 2022.)

Anzalone, C. 2020. Addressing the Enemy: Al-Shabaab's Psyops Media Warfare. *Combating Terrorism Center at West Point* 13,3: 41. https://ctc.usma.edu/addressing-enemy-al-shabaabs-psyops-media-warfare/

Aoláin, F.N. 2018. *Mandate of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism: Ol Oth 46/2018*. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. Available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/OL_OTH_46_2018.pdf

ARTICLE19 2022. Somalia Drop Charges against Journalist and Support Free Speech. https://www.article19.org/resources/somalia-drop-charges-against-journalist (Accessed on 18 January 2023.)

ATMIS 2023a. *Atmis Hands over Maslah Forward Operating Base to the Federal Government of Somalia.* Available at: https://atmis-au.org/atmis-hands-over-maslah-forward-operating-base-to-the-federal-government-of-somalia

ATMIS 2023b. *Home - African Transition Mission in Somalia Atmis.* Available at: https://atmis-au.org (Accessed on 18 January 2023.)

AU 2022. Communique - 1112 2022. PSC/PR/COMM.1112 2022. https://www.peaceau.org/uploads/eng-communique-for-the-1112th-psc-meeting.pdf

Babbie, E. 2008. *The Basics of Social Research*. 4th Edition. Thompson Wadsworth.

Bickert, M. & B. Fishman 2017. *Hard Questions: How We Counter Terrorism*. Meta. https://about.fb.com/news/2017/06/how-we-counter-terrorism

BRICS 2018. 10th BRICS Summit: 2018 Johannesburg Declaration. BRICS Summit Declaration. Available at: https://www.gov.za/speeches/10th-brics-summit-johannesburg-declaration-27-jul-2018-0000 (Accessed on 15 January 2023.)

BRICS 2019. 11th BRICS Summit: 2019 Brasilia Declaration. BRICS Summit Declaration. Available at: http://www.brics.utoronto.ca/docs/191114-brasilia.html (Accessed on 15 January 2023.)

BRICS 2020a. 12th BRICS Summit: 2020 Moscow Declaration. BRICS Summit Declaration. Available at: http://www.brics.utoronto.ca/docs/201117-moscow-declaration.html (Accessed on 15 January 2023.)

BRICS 2020b. BRICS Counter-Terrorism Strategy. Available at: https://eng.brics-russia2020.ru/images/114/81/1148168.pdf (Accessed on 15 January 2023.)

BRICS 2021a. 13th BRICS Summit: 2021 New Delhi Declaration. BRICS Summit Declaration. Available at: http://www.brics.utoronto.ca/docs/210909-New-Delhi-Declaration.html (Accessed on 17 January 2023.)

BRICS 2021b. BRICS Counter Terrorism Action Plan. https://brics2021.gov.in/brics/public/uploads/docpdf/getdocu-52.pdf

BRICS 2021c. BRICS National Security Advisors' Meeting. Available at: https://brics2021.gov.in/nsa-meeting (Accessed on 15 January 2023.)

BRICS 2022a. The 14th BRICS Summit is Held: President Xi Jinping Chairs the Summit and Delivers Important Remarks. Available at: http://brics2022.mfa.gov.cn/eng/tpxw/202206/t20220627_10710505.html

BRICS 2022b. 14th BRICS Summit: 2022 Beijing Declaration. BRICS Summit Declaration. Available at: https://www.thepresidency.gov.za/content/14th-brics-summit-beijing-declaration (Accessed on 15 January 2023.)

BRICS 2022c. Previous Summits Blog. Available at: http://brics2022.mfa.gov.cn/eng/gyjzgj/ljldrhwjj (Accessed on 18 January 2023.)

Burke, J. 2022. Journalist under Strict Bail Terms in Somalia after Arrest in Crackdown. *The Guardian.* https://www.theguardian.com/world/2022/nov/24/journalist-under-strict-bail-terms-in-somalia-after-arrest-in-crackdown (Accessed on 15 January 2023.)

Burke, J. & A.A. Mumin 2017. Survivors of the Mogadishu Market Bomb: 'Our Life Is Destroyed. There Is No More to Say'. *The Guardian.* Available at: https://www.theguardian.com/world/2017/dec/19/mogadishu-market-bomb-somalia-militants-terror-attack (Accessed on 18 January 2023.)

Burke, J. & A.A. Mumin 2018a. 'We laugh, sing and play music': The rise of Mogadishu. *The Guardian.* Available at: https://www.theguardian.com/world/2018/jul/11/somalia-the-rise-of-mogadishu-artists-music-activists (Accessed on 19 January 2023.)

Burke, J. & A.A. Mumin 2018b. 'Whatever it takes': People Brave War in Yemen in Hope of Reaching Europe. *The Guardian.* Available at: https://www.theguardian.com/global-development/2018/nov/05/whatever-it-takes-people-brave-war-yemen-in-hope-of-reaching-europe (Accessed on 19 January 2023.)

Burke, J. & A.A. Mumin 2019a. Car Bomb Kills at Least 11 and Port Manager Shot Dead in Somalia. *The Guardian.* Available at: https://www.theguardian.com/world/2019/feb/04/car-bomb-kills-at-least-11-and-port-manager-murdered-in-somalia

Burke, J. & A.A. Mumin 2019b. 'I was prepared to die': Survivors Recount Chaos of Nairobi Attack. *The Guardian.* Available at: https://www.theguardian.com/world/2019/jan/16/kenyan-president-says-nairobi-attack-over-all-militants-killed-al-shabaab

Burke, J. & A.A. Mumin 2019c. Severe Hunger Threatens Millions in Somalia as Climate Emergency Deepens. *The Guardian.* Available at: https://www.theguardian.com/global-development/2019/aug/29/severe-hunger-threatens-millions-somalia-climate-emergency-deepens (Accessed on 19 January 2023.)

Burke, J. & A.A. Mumin 2019d. 'We have nothing': Somalia Floods Raise Spectre of Famine. *The Guardian.* https://www.theguardian.com/world/2019/nov/19/we-have-nothing-somalia-floods-raise-spectre-of-famine (Accessed on 19 January 2023.)

Burke, J. & A.A. Mumin 2020a. Mogadishu's Refugees 'Waiting for death' as Covid-19 Reaches Somalia. *The Guardian.*

https://www.theguardian.com/global-development/2020/mar/24/mogadishus-refugees-waiting-for-death-as-covid-19-reaches-somalia (Accessed on 19 January 2023.)

Burke, J. & A.A. Mumin 2020b. Somali Medics Report Rapid Rise in Deaths as Covid-19 Fears Grow. *The Guardian.* https://www.theguardian.com/world/2020/may/02/somali-medics-report-rapid-rise-in-deaths-as-covid-19-fears-grow (Accessed on 19 January 2023.)

Carthy, S.L. & K.M. Sarma 2021. Countering Terrorist Narratives: Assessing the Efficacy and Mechanisms of Change in Counter-Narrative Strategies. *Terrorism and Political Violence* 35,3: 569 – 593. http://doi.org/10.1080/09546553.2021.1962308

Channel Africa. 2022. Al-Shabab Rattled after Somalia Media Ban. *General News*. https://web.archive.org/web/20230307182303/http://www.channelafrica.co.za/sabc/home/channelafrica/news/details?id=12a0fdde-f35b-41e8-9e32-0653225242c7&title=Al-Shabab%20rattled%20after%20Somalia%20media%20ban

Chigudu, D. 2021. Al-Shabab and Fundamental Terrorism in Somalia: Threats to the Continent and Beyond. *IJRBS* 10,3: 412 - 418. https://doi.org/10.20525/ijrbs.v10i3.1106

CIMA. 2007. *Community Radio: Its Impact and Challenges to Its Development*. Working Group Report. https://www.cima.ned.org/wp-content/uploads/2015/02/CIMA-Community_Radio-Working_Group_Report_0.pdf

Clarivate. 2024. *Endnote*. In Version 20.5. Clarivate. https://endnote.com/

Cox, K., W. Marcellino, J. Bellasio, A. Ward, K. Galai, K., S. Meranto & G. Paoli 2018. *Social Media in Africa a Double-Edged Sword for Security and Development Executive Summary*. United Nations Development Program. https://www.undp.org/sites/g/files/zskgke326/files/migration/africa/UNDP-RAND-Social-Media-Africa-Executive-Summary_final_3-Oct.pdf

CPJ 2022. Cpj Joins Call for Somali Authorities to Drop All Charges against Journalist Abdalle Ahmed Mumin. https://cpj.org/2022/12/cpj-joins-call-for-somali-authorities-to-drop-all-charges-against-journalist-abdalle-ahmed-mumin (Accessed on 19 January 2023.)

Dokman, T. & T. Ivanjko 2020. *Open Source Intelligence (OSINT): Issues and Trends*. https://doi.org/10.17234/INFUTURE.2019.23

https://doi.org/10.17234/INFUTURE.2019.23

DPPA 2022. *Subsidiary Organs of the United Nations Security Council* [Fact Sheets.] United Nations Department of Political and Peacebuilding Affairs. https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/subsidiary_organs_factsheets_06nov22.pdf

FAO 2020. Leaving No One Behind: Radio Initiative Educates Farmers; Pastoralists and Fisherfolk across Somalia - Somalia. https://reliefweb.int/report/somalia/leaving-no-one-behind-radio-initiative-educates-farmers-pastoralists-and-fisherfolk

FAO 2022. Distance Learning Via Radio for Rural Communities in Somalia – Overcoming COVID-19 Restrictions through Adaptive Measures That Facilitate Access to Agricultural and Nutrition Knowledge. https://doi.org/10.4060/cb8326en

Gaswaga, D. 2013. The Definition of Terrorism. *The International Journal of Ethical Leadership* 2,15: 1 - 20. https://scholarlycommons.law.case.edu/ijel/vol2/iss1/15

GCCS. 2020. *The Strategy and its Review Process.* Blue Sky V,1. Global Center on Cooperative Security. http://www.jstor.org/stable/resrep27519.6

GIFCT. 2023. *Gifct | Global Internet Forum to Counter Terrorism*. https://gifct.org
(Accessed on 10 January 2023.)

Hassan, F., S.S. Othman, S.H. Yusoff, K. Ali, S.Z. Omar & A.A. Musaddad 2021. A Systematic Literature Review of Knowledge and Awareness on Terrorism. *European Proceedigns of the Social and Behavioural Sciences* 203 - 218. https://doi.org/10.15405/epsbs.2022.01.02.17

Haugstvedt, H. 2024. Still Aiming at the Harder Targets: An Update on Violent Non-State Actors Use of Armed Uavs. *Perspectives on Terrorism* 18,1: 132 - 143. https://www.jstor.org/stable/27301123

Helmus, T.C. & K. Klein 2018. *Assessing Outcomes of Online Campaigns Countering Violent Extremism: A Case Study of the Redirect Method*. RAND Corporation. https://doi.org/10.7249/RR2813

Hossain, M.S. 2015. Social Media and Terrorism: Threats and Challenges to the Modern Era. *South Asian Survey* 22: 136 - 155. https://doi.org/10.1177/0971523117753280

HRW 2022a. Joint Letter Regarding the Arbitrary Arrest, Detention and Persecution of Mr. Abdalle Ahmed Mumin. Human Rights Watch.

https://www.hrw.org/news/2022/12/12/joint-letter-regarding-arbitrary-arrest-detention-and-persecution-mr-abdalle-ahmed
(Accessed on 18 February 2023.)

HRW 2022b. Somalia Free Detained Journalist 'Abdalle Ahmed Mumin', Respected Media Rights Advocate, Jailed in Mogadishu. https://www.hrw.org/news/2022/10/14/somalia-free-detained-journalist

Hu, J. & Yu, R. 2021. The Effects of ICT-Based Social Media on Adolescents' Digital Reading Performance: A Longitudinal Study of Pisa 2009, Pisa 2012, Pisa 2015 and Pisa 2018. *Computers & Education* 175. https://doi.org/10.1016/j.compedu.2021.104342

IGAD SSP 2016. *Al-Shabaab as a Transnational Security Threat*. https://igadssp.org/index.php/documentation/4-igad-report-al-shabaab-as-a-transnational-security-threat

Interpol 2022. Our 19 Databases - Search. *Interpol.int*. https://www.interpol.int/en/How-we-work/Databases/Our-19-databases

IPI 2022. Ipi Joins Call for Somali Authorities to Drop Charges against Journalist Abdalle Ahmed Mumin. https://ipi.media/ipi-joins-call-for-somali-authorities-to-drop-charges-against-journalist-abdalle-ahmed-mumin
(Accessed on 18 January 2023.)

Jain, P.N. & A.S. Vaidya 2020. Analysis of Social Media Based on Terrorism – Review. *Vietnam Journal of Computer Science* 08,1: 1 - 21. https://doi.org/10.1142/S2196888821300015

Jihadist Use of Social Media – How to Prevent Terrorism and Preserve Innovation 2011. 1st Session. https://www.govinfo.gov/content/pkg/CHRG-112hhrg74647/html/CHRG-112hhrg74647.htm

Klausen, J. 2015. Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. *Studies in Conflict & Terrorism* 38,1: 1 - 22. https://doi.org/10.1080/1057610X.2014.974948

Klausen, J. 2016. *The Role of Social Networks in the Evolution of Al Qaeda-Inspired Violent Extremism in the United States, 1990 - 2015*. NIJ/OSP U.S. Department of Justice. https://www.ojp.gov/ncjrs/virtual-library/abstracts/role-social-networks-evolution-al-qaeda-inspired-violent-extremism

Macdonald, S., S.G. Correia & A.-L. Watkin 2019. Regulating Terrorist Content on Social Media: Automation and the Rule of Law. *International Journal of Law in Context* 15,2: 183 - 197.

https://doi.org/10.1017/S1744552319000119

McDermott, Y., A. Koenig & D. Murray 2021. Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations. *Journal of International Criminal Justice* 19,1: 85 - 105. https://doi.org/10.1093/jicj/mqab006

Meta. 2016. *Partnering to Help Curb Spread of Online Terrorist Content*. Meta. https://about.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/

Meta. 2022. *Meta Launches New Content Moderation Tool as it Takes Chair of Counter-Terrorism Ngo.* Meta. https://about.fb.com/news/2022/12/meta-launches-new-content-moderation-tool (Accessed on 19 January 2023.)

Meta. 2023. *Dangerous Individuals and Organisations*. Transparency Centre. https://transparency.fb.com/de-de/policies/community-standards/dangerous-individuals-organizations (Accessed on 19 Janaury 2023.)

MIS [@MOISOMALIA.] 2022a. *Mogadishu, 12 October 2022: The Ministry of Information, Culture and Tourism Reaffirms.* [Tweet.] https://twitter.com/MOISOMALIA/status/1580453066985201665

MIS [@MOISOMALIA.] 2022b. *Press Release - Mogadishu, October 08, 2022.o.* [Facebook post.] https://www.facebook.com/moisomalia/posts/pfbid0pJtXRX4XEGy7moR3frYifGkNv6FGRSGNFjQsaaCuowfrPnt7yVj5pPDDy1s9QXBwl?__tn__=-R (Accessed in 2023.)

MIS [Ministry of Information of Somalia] 2022c. *Press Release: 12 October 2022.* [Facebook Post.] https://www.facebook.com/photo.php?fbid=442277091354673&set=a.260006176248433&type=3&theater

MIS [Ministry of Information of Somalia] 2023. *Government Communication Coordination Meeting* [Facebook post.] Ministry of Information – Somalia. [Facebook Page.] https://www.facebook.com/moisomalia/posts/pfbid0D2crNtxEXdnFwpcc142mSCmjQNhSBxEEtTEm7R8RnH4mozE8KkyU9NixFFomgy8zl?__tn__=-R

Moonshot. n.d. The Redirect Method - Moonshot. *Moonshot*. https://moonshotteam.com/the-redirect-method/

Mumin, A.A. 2018. Life at the Bottom of the Global League of Internet Access. *The Guardian.* https://www.theguardian.com/technology/2018/oct/18/life-at-the-bottom-of-the-global-league-of-internet-access

(Accessed on 18 January 2023.)

Oduoye, M.O., B. Javed, N. Gupta & C.M.V. Sih 2023. Algorithmic Bias and Research Integrity: The Role of Nonhuman Authors in Shaping Scientific Knowledge with Respect to Artificial Intelligence: A Perspective. *Internaitonal Journal of Surger* 109: 10. https://doi.org/10.1097/JS9.0000000000000552

OHCHR 2023a. *Annual Reports to the Human Rights Council and General Assembly*. United Nations Office of the High Commissioner Human Rights | Special Rapporteur on Counter-terrorism and Human Rights. https://www.ohchr.org/en/special-procedures/sr-terrorism/annual-reports-human-rights-council-and-general-assembly

OHCHR 2023b. *OHCHR | International Standards on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*. United Nations Office of the High Comissioner for Human Rights | Special Rapporteur on Counter-terrorism and Human Rights. https://www.ohchr.org/en/special-procedures/sr-terrorism/international-standards-promotion-and-protection-human-rights-and-fundamental-freedoms-while
(Accessed on 11 January 2023.)

OHCHR n.d. *Terrorism and Violent Extremism*. United Nations. https://www.ohchr.org/en/topic/terrorism-and-violent-extremism

PEN International 2022. Pen International Joins Other Human Rights Organisations Condemning the Persecution of Somali Journalist, Abdalle Ahmed Mumin. https://pen-international.org/news/pen-international-condemns-the-persecution-of-somali-journalist-abdalle-ahmed-mumin
(Accessed on 19 January 2023.)

Pledger, T.G. 2021. The Role of Drones in Future Terrorist Attacks. *Land Warfare* 137: 1 - 10. https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf

RFKHR 2023. *Rfk Human Rights Demands Release of Somali Journalist Abdalle Ahmed Mumin | Rfk Human Rights*. https://rfkhumanrights.org/press/robert-f-kennedy-human-rights-demands-immediate-release-of-somali-journalist-and-human-rights-defender-abdalle-ahmed-mumin (Accessed on 19 January 2023.)

RSF 2023. *Index*. Reporters Without Borders. https://rsf.org/en/index
(Accessed on 18 January 2023.)

Salkind, N.J. 2010. *Encyclopedia of Research Design.* Volume 1. SAGE Publications, Inc. https://doi.org/10.4135/9781412961288 PMid:20697321

Senekal, B. & E. Kotzé 2019. Open Source Intelligence (OSINT) for Conflict Monitoring in Contemporary South Africa: Challenges and Opportunities in a Big Data Context. *African Security Review* 28,1: 19 - 37. https://doi.org/10.1080/10246029.2019.1644357

Sheik, L. 2017. *Decoding News and Reception: An Investigation into the Discourses on Selected Facebook News Sites around Reports of the South African Farmland Attacks 2017 to 2018).* University of KwaZulu-Natal.

Sheikh, A. 2023a. *At Least Five Injured after Blast at Mayor's Office in Mogadishu*. Reuters. https://www.reuters.com/world/africa/blast-heard-near-mayors-office-somalias-capital-mogadishu-witness-2023-01-22/ (Accessed on 17 January 2023.)

Sheikh, A. 2023b. Death Toll Rises to 35 after Al-Shabaab Car Bomb Attack in Central Somalia. *Hiiraan Online.* https://www.hiiraan.com/news4/2023/Jan/189343/death_toll_rises_to_35_after_al_shabaab_car_bomb_attack_in_central_somalia.aspx (17 Janaury 2023.)

Sheppard, V. 2020. *Research Methods for the Social Sciences: An Introduction*. BCCampus Pressbooks. https://pressbooks.bccampus.ca/jibcresearchmethods/

Sims, A. 2018. The Rising Drone Threat from Terrorists. *Georgetown Journal of International Affairs* 19: 97 - 107. https://www.jstor.org/stable/26567532; https://doi.org/10.1353/gia.2018.0012

SMF 2022. *What Are the Challenges and Limitations of Private Social Media Companies in Cleaning up Illicit Content Online in Their Role as Agents of Counter-Terror?* https://sjsyndicate.org/wp-content/uploads/2022/10/Joint-Statement-Somali-media-fraternity-expresses-concern-about-the-Somalia-government%E2%80%99s-directive.pdf

SMSJ 2021. *Journalists Safety and Media Freedom in Somalia*. https://www.mediasupport.org/wp-content/uploads/2022/06/Journalists-Safety-and-Media-Freedom-in-Somalia.pdf

Snyder, H. 2019. Literature Review as a Research Methodology: An Overview and Guidelines. *Journal of Business Research* 104: 333 - 339. https://doi.org/10.1016/j.jbusres.2019.07.039

SONNA [@SONNALIVE.] 2022. *Disseminating Extremism Ideology Is Recognized as a Crime.* [Tweet.] https://twitter.com/SONNALIVE/status/1578774905986093056 (Accessed on 08 October 2023.)

Terrorism and Social Media:#Isbigtechdoingenough? 2018. 2nd Session. https://www.govinfo.gov/content/pkg/CHRG-115shrg31316/html/CHRG-115shrg31316.htm

Ucko, D.H. 2018. Preventing Violent Extremism through the United Nations: The Rise and Fall of a Good Idea. *International Affairs* 94,2: 251 - 270. https://doi.org/10.1093/ia/iix235

UKZN 2020. *Apa 7th Edition Style Print and Online Sources.* https://web.archive.org/web/20230726142826/https://libguides.ukzn.ac.za/ld.php?content_id=55781705

UN 2020. *Leaving No One Behind: Radio Initiative Educates Farmers; Pastoralists and Fisherfolk across Somalia*. United Nations Somalia. https://somalia.un.org/index.php/en/106702-leaving-no-one-behind-radio-initiative-educates-farmers-pastoralists-and-fisherfolk-across (Accessed on 28 January 2023.)

UN 2022. Un Security Council Boosts Commitment to Fight Digital Terror. *UN News: Global Perspective Human Stories*. https://news.un.org/en/story/2022/10/1130007 (Accessed on 19 January 2023.)

UN 2023a. *The 17 Goals : Sustainable Development*. https://sdgs.un.org/goals

UN 2023b. *Main Bodies | United Nations*. United Nations. https://www.un.org/en/about-us/main-bodies#:~:text=The%20main%20bodies%20of%20the,Organization%20was%20founded%20in%201945 (Accessed on 18 January 2023.)

UNCTC 2022. *Delhi Declaration on Countering the Use of New and Emerging Technologies for Terrorist Purposes*. UNCTC. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_special_meeting_outcome_document.pdf (Accessed on 14 January 2023.)

UNGA 2006a. Protection of Human Rights and Fundamental Freedoms While Countering Terrorism. [UN General Assembly Resolution.] *A/61/267*. https://digitallibrary.un.org/record/583710?ln=en

UNGA 2006b. The United Nations Global Counter-Terrorism Strategy. [UN General Assembly Resolution.] *A/RES/60/288*. https://undocs.org/A/RES/60/288

UNGA 2015. Plan of Action to Prevent Violent Extremism. [UN General Assembly Resolution.] *A/70/674*. https://digitallibrary.un.org/record/816212

UNGA 2019. Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism: Note by the Secretary-General. [UN General Assembly Resolution.] *A/74/335*. https://undocs.org/A/74/335

UNGA 2021. The United Nations Global Counter-Terrorism Strategy: Seventh Review. [UN General Assembly Resolution.] *A/RES/75/291*. https://undocs.org/A/RES/75/291

UNODC 2017. *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System* Vol. UN Global Programme to End Violence against Children. United Nations Office on Drugs and Crime UNODC. https://www.unodc.org/documents/justice-and-prison-reform/Child-Victims/Handbook_on_Children_Recruited_and_Exploited_by_Terrorist_and_Violent_Extremist_Groups_the_Role_of_the_Justice_System.E.pdf

UNSC 2004. Resolution 1566 2004. [UN Security Council Resolution.] *S/RES/1566 (2004)*. http://undocs.org/en/S/RES/1566 (2004)

UNSC 2017a. Comprehensive International Framework to Counter Terrorist Narratives. [UN Security Council Resolution.] *S/2017/375*. https://undocs.org/S/2017/375

UNSC 2017b. Resolution 2354 (2017) [UN Security Council Resolution.] *S/RES/2354 2017*. https://undocs.org/S/RES/2354 (2017)

UNSC 2022a. *Meetings Coverage: Unanimously Adopting Resolution 2628*. https://press.un.org/en/2022/sc14847.doc.htm

UNSC 2022b. Resolution 2628 (2022) [UN Security Council Resolution.] *S/RES/2628 (2022)*. https://undocs.org/en/S/RES/2628 (2022)

UNSOM 2017. *Countering Al-Shabaab Propaganda and Recruitment Mechanisms in South Central Somalia*. UN. https://reliefweb.int/report/somalia/countering-al-shabaab-propaganda-and-recruitment-mechanisms-south-central-somalia

Yeboah-Ofori, A. 2018. Cyber Intelligence and Osint: Developing Mitigation Techniques against Cybercrime Threats on Social Media. *International Journal of Cyber-Security and Digital Forensics* 7: 87 - 98. https://doi.org/10.17781/P002378

Zanasi, F. & F. Ruini 2018. IT-Induced Cognitive Biases in Intelligence Analysis: Big Data Analytics and Serious Games. *International Journal of Safety and Security Engineering* 8,3: 438 - 450. https://doi.org/10.2495/safe-v8-n3-438-450

Professor Nirmala Devi Gopal
Criminology & Security Studies
Department of Criminology & Forensic Studies
Howard College Campus
University of KwaZulu-Natal
Durban, South Africa
Gopal@ukzn.ac.za

# Chapter 8: A Survey of Cybersecurity Issues in BRICS Countries – A Systematic Review

**Oluwafisayo Kaka**

## Abstract

**Purpose:** This paper aims to assess cybersecurity issues within BRICS countries and identify policies and measures used to tackle identified cyberattacks.

**Background:** Cybercrime is a global issue, that affects all facets of the society. Criminals conduct cyberattacks for diverse reasons such as stealing information, monetary gain, identity theft and to attack critical infrastructure. The association of Brazil, Russia, India, China and South Africa called BRICS, is considered a group of emerging developing countries with progressive financial growth. The financial development of these countries has made them better targets for cybercriminals. Hence, each country within BRICS responds to cyberattacks using set policies and standards according to existing and new cyber threats within their borders.

**Method**: The researcher conducted a systematic review of existing literature on the topic, gathering information from peer-reviewed journals, government documents, reports, policy documents, and other relevant documents on cybersecurity responses of BRICS countries. The selected documents were then analysed.

**Contribution**: Cyberattack responses are crucial to safeguarding citizens, businesses, organisations, and assets of a nation. The continuous advancement in technology creates more ways to attack, causing issues such as data breaches, financial theft, and political goals. Hence, it is important to assess how these

AASBS Volume #21 (2025) https://doi.org/10.29086/978-0-9869938-0-0/2025/AASBS21
Chapter DOI: https://doi.org/10.29086/978-0-9869938-0-0/2025/AASBS21/8 pp. 187 - 221

issues are currently tackled to implement better measure thereby reducing the success rate of cyberattacks. BRICS nations can benefit from using the result of this research to improve existing cybersecurity policies and solutions.

**Findings**: The study findings indicated that some cybersecurity policies and regulations are dated and may not be effective when implemented against sophisticated cyberattacks. Skill gaps also exist in the cybersecurity field which leaves a few professionals available to respond to cyberattacks. In addition, there is little cybersecurity collaboration between governments and private organisations.

**Recommendations:** To reduce the success rate of cyberattacks, the government of each BRICS country can work alongside private firms to establish better policies and procedures internally. The study also recommends collaboration within the BRICS association by sharing and adopting best cybersecurity practices by each nation. Furthermore, priority should be given to training and recruiting more cybersecurity professionals from these nations.

**Impact on Society**: Cyberattacks are a global problem. Thus, it is essential to establish effective solutions to reduce the problem in society. Resolving cybersecurity issues enables better information security, privacy, and physical and digital asset protection.

**Future Research**: Future research can focus on nationwide studies from each BRICS nation to provide an in-depth insight into the effectiveness of existing cybersecurity policies and current implementation measures. The outcome can help to replace ineffective cybersecurity solutions with effective ones.

**Keywords:** BRICS, Cybersecurity, Cyberattacks, Regulations and Policies

## Introduction

In today's digital age, the Internet plays an important role in our daily lives in areas such as work, education, communication, leisure, and health. However, our dependence on the Internet also creates opportunities for cyberattacks (Saleous, Ismail, AlDaajeh, Madathil, Alrabaee, Choo & Al-Qirim 2023). BRICS countries, comprising Brazil, Russia, India, China, and South Africa,

have emerged as significant countries in digital and economic transformation among developing nations (UNDP 2022). The countries are home to more than 40% of the world's population. In addition, these nations have become innovation and technology hubs with great economic feats, making them attractive targets for cybercriminals (Belli, Gaspar & Jaswant 2024; World Economic Forum 2021). The combined GDP of BRICS countries is approximately 29% of the world's GDP (Chen, Dao & Nhieu 2024). Despite this feat, BRICS nations do not have consistent economic growth annually but rather have a level of economic consistency, with a projected growth of 4% (IMF 2023). In 2023, the BRICS group were regarded as high cyber risk area of the world, with the cyber risk rate as follows: China 49.5%, South Africa 48.6%, while India, Brazil and Russia had 47.9%, 44% and 43.9% respectively (Checkpoint 2023).

The cybercrime index of 2024 indicated that all BRICS countries are ranked in the top fifteen countries that are hot spots for cybercrimes. The current ranking is as follows: Russia, China, Brazil, India and South Africa in numbers one, three, nine, ten and fourteen respectively (Bruce, Lusthaus, Kashyap, Phair & Varese 2024). In addition, Cybercrime as a Service (C.a.a.S.) is increasing due to more demand for online services that enable cybercrimes, and this is a threat to people worldwide (Microsoft 2023). Cybersecurity threats can occur in many forms, including hacktivism, phishing, malware, and DDoS attacks. Cyberattacks are costly to economies (World Economic Forum 2021).

Several high-profile cybercrimes have affected these countries in recent years. The attack on the Indian power grid through network intrusion is an example (Dutta 2021). The theft of over $3 billion from Brazilian banks in 2018 is another instance (RSA 2014). Additionally, China experienced the remote control of over one million IP addresses, the hijack of forty-two thousand websites by hackers in 2009 (Kshetri 2013), and the theft of South African bank details in 2019 during a mega-chart attack (Accenture 2020). These further showcase the vulnerability of the BRICS nations to cyberattacks.

These incidents of cybercrime have caused significant damage to the reputation of these countries and hurt their investment climate (World Economic Forum 2020a). To handle these issues, the BRICS nations have committed to the creation of a unified and practical solution to cyberattacks through the XIV BRICS Summit Beijing Declaration during its June 2022 summit (Xinhua 2022). Each country has laws and regulations to ensure information and data protection (Belli 2021a).

## Global Cybersecurity Incidents and Responses

A cyber threat is any attempt to damage, disrupt, or gain unauthorised access to data and resources on a computer system or network. Threats online can occur in many forms, including malware (Saleous *et al*. 2023), phishing attacks, ransomware, data loss, and identity theft (Alkhalil, Hewage, Nawaf & Khan 2021). According to Gartner, the global expenditure on risk management and information security was estimated to be $185 billion in 2023 (Gartner 2024). Global cyberattacks increased by 28% in 2024 (Checkpoint 2024). Indicating that no country is immune to cybercrime, as demonstrated by the United States, which has experienced some of the worst cyberattacks in history. The United States was ranked number one worldwide for global DDoS attack destinations with a 55% risk rate (Microsoft 2023).

Another major form of cyberattack is hacktivism which is used today. The attacker uses hacking for political or social reasons, targeting organisations or entities with which the attackers disagree. It is sometimes seen as an act of terrorism (Romagna 2020). An example of this is the 2012 attack by Anonymous on the website of the United States Department of Justice in response to the shutdown of the file-sharing website Megaupload (Bellaby 2021). These cyberattacks have created major concerns, as hacktivism is increasing, especially between countries such as Russia and Ukraine engaged in political conflicts (Checkpoint 2024). This puts businesses, governments, and individuals at risk. This has led to collaboration between the United States government and private organisations in the country to address the problem. Organisations are also encouraged to disclose newly discovered malware to the government (Neuberger, Zegart & Segal 2021a).

In terms of national implementation, countries are taking various approaches to address cybersecurity. For instance, the United States municipalities have cybersecurity practices included in the process management of data and likewise conduct training on data security. The United Kingdom government has cross-sector Critical National Infrastructure (C.N.I.) services that manage cybersecurity issues (Shukla, Johnson & Jones 2019; Hatcher, Meares & Heslen 2020). European countries also have a baseline risk management and reporting method in place to strengthen cybersecurity in the region. Australia on the other hand, passed a new law to protect its citizens from online fraud by introducing a penalty of $50 million for criminals that conduct online fraud. Singapore created an inter-agency task force to tackle ransomware and cybercrimes (Checkpoint 2023). Countries like China and Russia have

integrated cybersecurity into their national security strategies because both countries are cyber-ambitious (Kshetri 2016; Jiang 2021).

Several global initiatives and organisations have been established to address the issue of cybersecurity, such as the establishment of the International Telecommunication Union (I.T.U.). ITU is a specialised agency of the United Nations that deals with information and communication technologies. The ITU has developed recommendations and guidelines for cybersecurity, such as the ITU-T X.805 series of recommendations on security in telecommunications networks (Mix 2022). Additionally, the Global Cybersecurity Index (G.C.I.) is a tool developed by the ITU to measure the commitment of countries to handle cybersecurity. The GCI provides a benchmark for countries to assess their level of cybersecurity development and compare it to other countries. The index is based on five pillars: legal, technical, organisational, capacity building, and cooperation (ITU 2020). The GCI is widely used by countries and organisations to assess cybersecurity readiness and identify areas for improvement. According to a survey conducted by the World Economic Forum (W.E.F.), 42% of cyber leaders identified infrastructure breakdown due to cyberattacks as a major concern, followed by identity theft at 24%, and 20% were concerned about ransomware attacks (World Economic Forum 2021). The private sector also plays a significant role in implementing cybersecurity measures globally, with companies such as Microsoft and Cisco Systems developing products and services to help organisations protect their networks and systems from cyberattacks (Microsoft 2023; Rawindaran, Jayal, Prakash & Hewage 2021). Several international standards are likewise widely used for cybersecurity, such as ISO/IEC 27001, the National Institute of Standards and Technology (N.I.S.T.), Cybersecurity Framework (C.S.F.) and the Control Objectives for Information and Related Technologies (C.O.B.I.T.) (Mix 2022). The Organisation for Economic Cooperation and Development (O.E.C.D.) also developed guidelines for the security of information systems and networks (Eldem 2021).

The cybersecurity problems and solutions of each country differs to some extent, which indicates the necessity to understand cyberattacks and the associated responses considering the following: the existing cybersecurity policies and measures of BRICS countries and the impact of these measures. Understanding these will provide appropriate recommendations to noted challenges. Furthermore, to achieve these objectives, available literature, research findings, security reports, records on cyberattacks and measures in BRIC countries were diligently studied.

## Research Methodology

To answer the research question of this exploratory study, information was primarily deduced from the information security field. A systematic review was conducted on peer-reviewed journal articles, government reports, policy documents and other relevant documents that discuss cybersecurity responses of BRICS countries. Using the systematic review is due to a lack of access to classified government statistical reports and information which are not privy to public access. The review of existing literature however enables the examination of relevant information on the research topic while noting the major questions surrounding the topic. In addition, the review identifies documented research gaps that can be further explored. Research experts on the topic are also discovered in the process of the review, therefore guiding the researcher's focus during the study. The challenge experienced during systematic review is the time it takes to search for specific information on the research topic. This can lead to the use of advanced filter searches to accommodate extensive keyword searches from dedicated journal platforms and research databases. The researcher used platforms such as informational portals,

IEEE, ACM, EBSCO, Science Direct, Government portals and websites, and Google Scholar to gather relevant publications on the cybersecurity responses of BRICS countries. The selected documents were published within the last twenty years because some cybersecurity policies were established during the early era of the Internet. Similarly, certain past cyberattacks were influential in the development of cybersecurity measures noted today. Of the utilised papers, 66 out of 78 could be used for the study's analysis.

## Process and Eligibility Criteria

The review of the literature of this paper is based on the findings of existing research published in journals, online databases containing empirical works, and reports that analysed cybersecurity responses of the countries within the BRICS association. The outline of this systemic review is focused on Preferred Reporting Items for Systematic Reviews and Meta-Analyses statements (Page *et al.* 2021).

## Inclusion and Exclusion Criteria

The search keywords were restricted to the 'Information security' discipline. The data extraction used the following keywords such as 'Cybersecurity in BRICS', 'China', 'Russia', 'India', 'Brazil' and 'South Africa' as indicated in Table 1 below. For the gathered data to be eligible for use, the previously mentioned keywords were used as a screening criterion. Documents that had those keywords missing and literature not written in English were excluded from the research as depicted in Figure 1.

**Table 1: Search terms used in the systematic review**

| Keyword Category | Search terms |
|---|---|
| Cybersecurity in BRICS | Cybersecurity policies in BRICS countries.<br>Cybersecurity measures in BRICS countries. |
| Brazil | Cybersecurity in Brazil.<br>Cyberattacks in Brazil.<br>Cybersecurity policies in Brazil. |
| Russia | Cybersecurity in Russia.<br>Cyberattacks in Russia.<br>Cybersecurity policies in Russia. |
| India | Cybersecurity in India.<br>Cyberattacks in India.<br>Cybersecurity policies in India. |
| China | Cybersecurity in China.<br>Cyberattacks in China.<br>Cybersecurity policies in China. |
| Africa | Cybersecurity in South Africa.<br>Cyberattacks in South Africa.<br>Cybersecurity policies in South Africa. |

To derive useful information from documents, a document analysis was conducted. This form of analysis is a qualitative method used to review existing documents in the study area. The qualitative analysis requires coding the answers under the theme of the research topic (Bowen 2009). Thematic analysis interprets the insight into a meaningful output while providing empirical

information (Maguire & Delahunt 2017). For information analysis, inductive and deductive reasoning were utilised by assessing and producing useful output from the reviewed documents (Tie, Birks & Francis 2019).

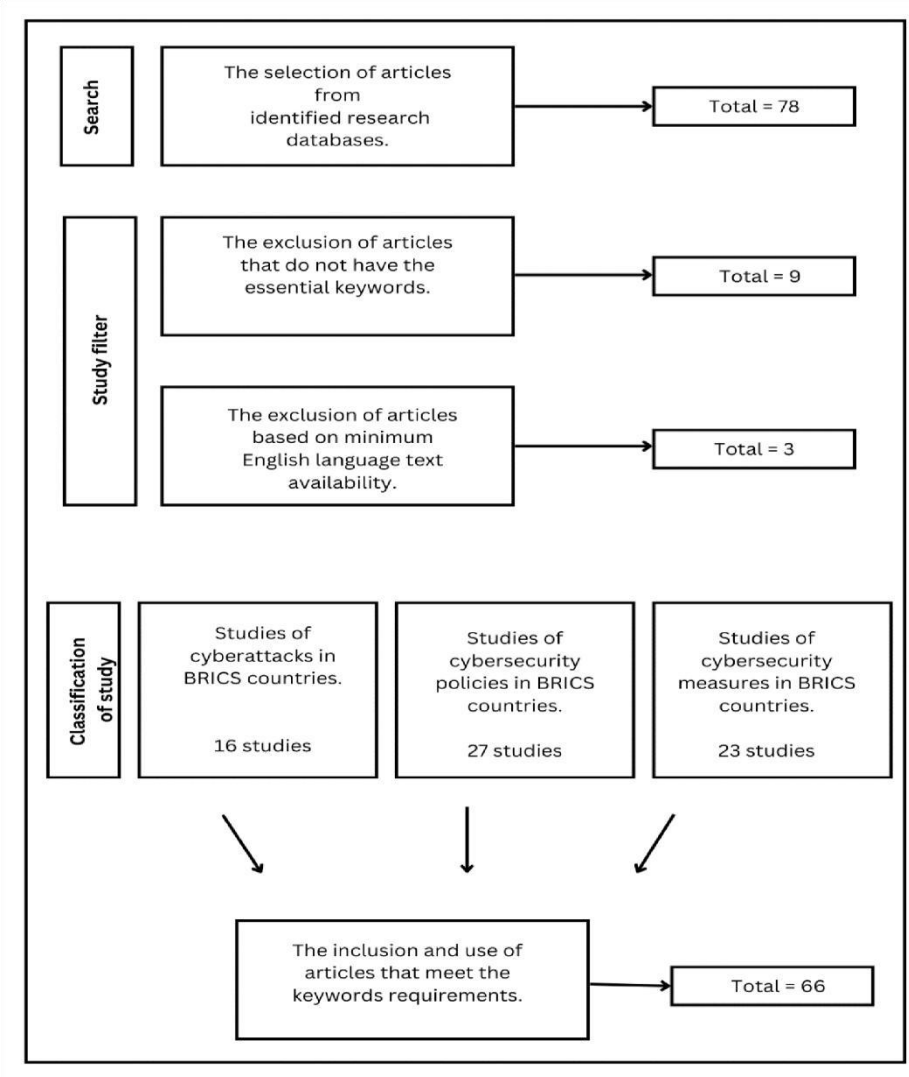



**Figure 1: Phases in the literature selection process**

For insightful deduction, the researcher analysed articles cited numerous times that met the selection criteria and data was collected for analysis**.** Past studies, indicates that articles cited numerous times are insightful and can provide good theoretical information and research methodology while exposing research gaps yet to be explored (Dalglish, Khalid & McMahon 2020).

Figure 2 as shown below indicates the percentage of useful articles and other relevant documents used in this study according to the range of years considered 2000 till date. The selected range of publications is because some legal documents and other relevant articles exist within that timeframe. The percentage of useful articles is not significantly high due to the publications that focus on the research topic, showing, 66 out of 78. This outlines a low publication on this topic between the year 2022 to 2024 indicating fewer current statistics and articles.

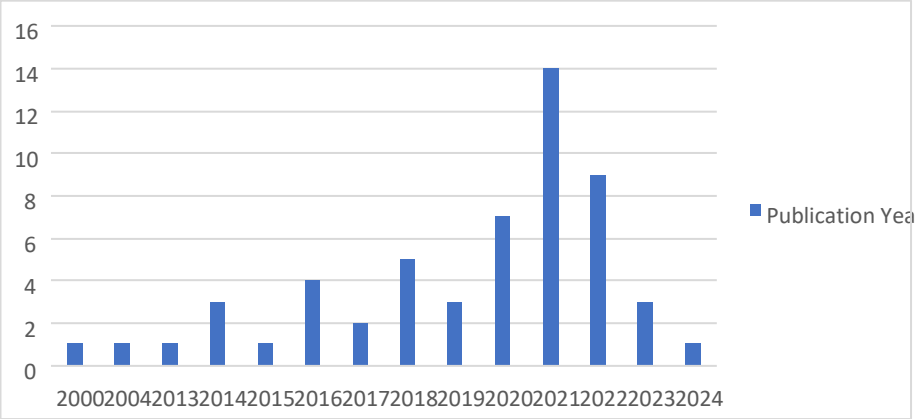



**Figure 2: Distribution of the research papers by year**

## Data Extraction and Synthesis

The researcher independently extracted data from the chosen research documents using the following criteria:

Does the paper identify existing cybersecurity issues among BRICS countries? Does the paper identify existing cybersecurity policies among BRICS countries? Does the paper assess the cybersecurity measures used by each BRICS nation?

The extracted data was accessed by an independent assessor invited by the researcher to review the selected documents for any discrepancies (Mallett, Hagen-Zanker, Slater & Duvendack 2012). Any differences were resolved through consensus to establish consistency in data collection and quality assurance tailored to address the theme of the study: cybersecurity issues in BRICS countries.

## Findings and Results

The results from the reviewed papers are presented in this section. The paper synthesis assessed different perspectives on the cybersecurity problems experienced in BRICS countries in the past and recent times while examining what security measures have been implemented by each nation. Table 2 presents the reviewed papers mapped to the cybersecurity issues experienced by BRICS countries.

Table 3 and Table 4 present the data on cybersecurity policies and measures established and implemented by each BRICS nation. Afterwards, the findings are discussed, and recommendations are provided to solve the existing cybersecurity issues in the studied BRICS countries.

**Table 2: Mapping of reviewed papers on past cyberattacks experienced in BRICS countries**

| Table 2 | Past cyberattacks experienced in BRICS countries | | |
|---|---|---|---|
| **Study** | **Malware** | **Phishing** | **DDoS** |
| Alkhalil *et al.* (2021) | X | | |
| Bellaby (2021) | X | | |
| Botacin *et al.* (2021) | | X | |
| Checkpoint (2024) | X | | |
| Gartner (2018) | X | | |
| Jie & Lin (2021) | | X | |
| Kshetri (2013) | | | |
| Kumar & Singh (2020) | | X | |
| Meyers (2018) | | X | |

| | | | |
|---|---|---|---|
| Microsoft (2023) | | | X |
| Pieterse (2021) | X | | |
| SARS (2022) | | X | |
| Singer & Friedman (2014) | X | | |
| Van Niekerk (2017) | | | X |
| Vaz Ferreira (2022) | X | | |
| Zieni, Massari & Calzarossa (2023) | | X | |

**Table 3: Mapping of reviewed papers on cybersecurity policies implemented by each BRICS country**

| Table 3 | Cybersecurity policies implemented by each BRICS country | | | | |
|---|---|---|---|---|---|
| **Study** | **Brazil** | **Russia** | **India** | **China** | **South Africa** |
| Al- Qahtani & Cresci (2022) | | X | | | |
| Belli (2021a) | X | X | X | X | X |
| Belli (2021b) | X | X | X | X | X |
| Dlamini & Mbambo (2019) | | | | | X |
| Endeshaw (2004) | | | | X | |
| Gritsenko, Wijermars & Kopotev (2021) | | | X | | |
| Hurel & Lobato (2018) | X | | | | |
| Hurel (2021) | X | | | | |
| Hurel (2022) | X | | | | |
| Johnson, Lincke, Imhof & Lim (2014) | X | | | | |
| KPMG (2016) | | | | X | |
| KPMG (2021) | | | X | | |
| Kshetri (2016) | | X | | | |
| Li (2015) | | | | X | |

| | | | | | |
|---|---|---|---|---|---|
| Miao *et al.* (2021) | | | | X | |
| Netshakhuma (2022) | | | | | X |
| Neuberger, Zegart & Segal (2021a) | | | X | | |
| Oppermann (2014) | X | | | | |
| Phahlamohlaka (2022) | | | | | X |
| PWC (2018) | | | | X | |
| Qiu (2000) | | | | X | |
| Radebe *et al.* (2022) | | | | | X |
| Sethi (2020) | | | X | | |
| Shvets (2020) | | X | | | |
| Veiga (2022) | | | | | X |
| Wei (2020) | | | | X | |
| Zdziarski (2018) | | X | | | |

**Table 4: Mapping of reviewed papers on cybersecurity measures implemented by each BRICS country**

| Table 4 | Cybersecurity measures implemented by each BRICS country | | | | | |
|---|---|---|---|---|---|---|
| **Study** | **BRICS Cyber-security Measures** | **Brazil** | **Russia** | **India** | **China** | **South Africa** |
| Al-Qahtani & Cresci (2022) | | | X | | | |
| Belli (2021b) | X | X | X | X | X | X |
| Cary (2021) | | | | | X | |
| Chen (2021) | | | | | X | |
| Chen & Sun (2021) | | | | | X | |
| Chen, Wu & Liu (2020) | | | | | X | |
| Connell & Vogler (2016) | | | X | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Costa *et al.* (2022) | | X | | | | |
| Dlamini & Mbambo (2019) | | | | | | X |
| Gritsenko, Wijermars & Kopotev (2021) | | | X | | | |
| Hurel (2021) | | X | | | | |
| Hurel & Lobato (2021) | | X | | | | |
| ISACA (2023) | X | | | | | |
| Neuberger, Zegart & Segal (2021b) | | | X | | | |
| Pursiainen (2020) | | | X | | | |
| Radebe *et al.* (2022) | | | | | | X |
| Romaniuk & Manjikian (2020) | | | | | | X |
| Singh (2019) | | | | X | | |
| Stadnik (2019) | | | X | | | |
| Sutherland (2017) | | | | | | X |
| Thakral *et al.* (2016) | | | | X | | |
| Urbanovics (2022) | | X | | | | |
| Xulu (2022) | | | | | | X |

## Cyberattacks that Prevalently Affect Each BRICS Country

Specify types of cyberattacks are more successful in certain countries and BRICS countries are not exceptional to such attacks. According to the 2024 cybersecurity index, cybercriminals in Russia specialise in sophisticated cybercrimes. China and Brazil will see more technically complex attacks such as data and identity theft, while India and South Africa experience more high and low-tech crimes. For example, scams are a common form of cyberattack in India (Bruce, Lusthaus, Kashyap, Phair & Varese 2024). The cyberattacks below are fairly common in BRICS countries.

## *Malware*

Malware, also known as malicious software, is a program created to harm or disrupt the computer system of a victim. Some common types of malware include but are not limited to, viruses, worms, trojans, and ransomware that can be installed on a computer without the victim's knowledge to steal information or damage data (Aslan & Samet 2020). According to Checkpoint's threat report for the past year, multipurpose malware is the leading by 31% against other forms of threats (Checkpoint 2024). In 2014, it was reported that China experienced a high level of malware infection owing to the wide use of pirated software on computers (Singer & Friedman 2014). In 2018, a ransomware attack affected several major corporations in Russia, resulting in widespread data loss and disruption (Gartner 2018). In 2016, a malware attack affected several banks in India, such as HDFC, ICICI and SBI where 3.2 million ATM cards were hacked to divert funds (Bellaby 2021). The Brazilian Supreme Court of Justice experienced a ransomware attack in 2020 causing major disruptions to its operations (Vaz Ferreira 2022). In 2019, Johannesburg, South Africa's electricity supply experienced two successive ransomware attacks, causing a widespread power outage in the city (Pieterse 2021).

## *Phishing*

Phishing is a type of cyberattack which uses psychological and social engineering methods to defraud victims. The attacker uses fake emails or websites to trick victims into revealing sensitive information such as passwords or credit card numbers. Thus, phishing is a method of defrauding people (Zieni, Massari & Calzarossa 2023). Attackers often use persuasive means to get reliable information from victims (Akdemir & Yenal 2021). Once attackers have this information, such criminals can use it to access accounts or commit identity theft (Shulzhenko & Romashkin 2020). In Brazil, phishing attacks often target the users of banking and government tax services. The country is an economic power among Latin American countries. In the past, criminals have created fake messages to deceive users into entering personal information on a malicious link. For instance, there was a taxpayer's scam in Brazil, where attackers used an annual government measure that required taxpayers to fill income forms through an online portal to redirect and collect legal information from late tax filers (Botacin, Aghakhani, Ortolani, Kruegel, Vigna, Oliveira, De Geus & Grégio 2021). In 2022, a phishing campaign was reported targeting South African bank customers, where attackers sent fake emails claiming to be

from the South African Revenue Service (S.A.R.S.), asking for personal information (SARS 2022).

Similarly, India experienced a rise in phishing attacks when the COVID-19 pandemic began, with the presence of fake websites, links and other deceptive measures to defraud and steal information from people (Kumar & Singh 2020). Russian banks and financial institutions were also attacked in 2018 when fake emails with malicious attachments that could steal sensitive information were sent to customers (Meyers 2018). The Chinese company Alibaba Group's customers experienced phishing attacks in 2019 when attackers sent fake emails asking customers to update their payment information (Jie & Lin 2021).

## Distributed Denial-of-Service (DDoS)

Distributed Denial-of-Service (D.D.o.S.) attacks are cyberattacks that aim to make a website or network unavailable by overwhelming it with traffic from multiple sources, often using botnets. Botnets are enduser computers or hosts that are maliciously affected on a network and controlled by a cybercriminal to conduct malicious actions (Alieyan, Almomani, Abdullah, Almutairi & Alauthman 2020). The South African mobile operator MTN experienced a DDoS attack in 2013, which led to service disruptions for customers (Van Niekerk 2017). In 2016, a major DDoS attack affected many digital devices in countries such as India, Brazil and China. The DDoS exploited the default login details of these devices and well-known websites (Belli 2021a). Microsoft's digital defence report of 2023 indicated that over 1700 DDoS attacks occur per day. The report ranked Russia, China and India in the top ten DDoS attack destinations globally, with an estimated attack rate of 14%, 7% and 4% respectively (Microsoft 2023).

## Cybersecurity Regulations and Policies Established by Each BRICS Country

BRICS nations have recognised the importance of cooperation in addressing cybersecurity issues such as data security and online content regulations. The 2022 Beijing BRICS declaration emphasised the importance of BRICS nations working together and addressing cybersecurity concerns such as cyber espionage, malware attacks, and other malicious activities (Republic of China

2022). To protect citizens and businesses, these nations have implemented a range of cybersecurity policies and strategies discussed below.

## *Brazil*

Brazil has taken significant steps to address cybersecurity incidents, such as the passing of cybercrime bills in 2012 to ensure the creation of dedicated units to combat cybercrime, handle data, and protect it. The establishment of the Information Security Policy and Information Security Steering Committee (C.G.S.I.), to handle information security issues (Johnson, Lincke, Imhof & Lim 2014; Oppermann 2014; Hurel & Lobato 2018). This is because cyberattacks in Brazil have resulted in considerable financial losses (Devanny, Goldoni & Medeiros 2022). Cybersecurity is included in the national security agenda of Brazil, including:

- The Digital Bill of Rights of 2013.
- The establishment of the Cyber Defense Center (C.D.Ciber.) is a joint effort between government and private organisations. This was done despite the country's digital inequality with Internet services.
- The Department of Computer Emergencies Response Team (D.E.C.R.T.) was created to handle such infrastructural problems (Hurel & Lobato 2018).

The country also has other laws and regulations to address cybersecurity, such as the Brazilian Civil Rights Framework for the Internet, the Brazilian General Data Protection Law, and the Brazilian Cybercrime Law (Belli 2021a). In addition, Brazil has a National Cybersecurity Plan launched in 2018 to reduce the number of cybersecurity incidents and improve the response to such incidents by establishing a framework for cooperation between the public and private sectors (Hurel 2021).

## *Russia*

Russia's cybersecurity laws and regulations include the Federal Law on information, information technologies and information protection. The Information Law was passed in 2000, to protect personal data and regulate the use of personal data. Russia's Federal Law on Personal Data was passed in

2006, which regulates the collection, storage, and use of personal data (Kshetri 2016; Shvets 2020; Zdziarski 2018). To further address cyber security attacks, Russia established the National Cyber Security Centre to implement the National Cyber Security Strategy and System and provide other solutions. In 2017, President Putin signed the National Cyber Security Strategy (Al-Qahtani & Cresci 2022), which outlined the country's goals and measures to protect citizens, sovereignty and others from cyberattacks. However, the effectiveness of these measures is a subject of debate as the country allegedly does statesponsored hacking as a form of defence. In addition, weak penalties, and inadequate and insufficient cybersecurity laws do not discourage online crimes as these problems persist (Kshetri 2016).

## *India*

To address cybersecurity, India has several laws and regulations in place, including:

- The Information Technology Act (I.T.A.) of 2000, criminalises hacking, identity theft, online fraud, and other cybercrimes and established a legal framework for electronic signatures and electronic documents (Sethi 2020).
- The 2009 Information Technology Rules of Guidelines for Cybercrime Investigation.
- The 2011 Information Technology Rules of Intermediaries Guidelines.
- The 2011 Information Technology Rules of Reasonable Security Practices and Procedures and Sensitive Personal Data or Information.
- The Cyber Security of Critical Information Infrastructure Protection Bill of 2013 (KPMG India 2021).
- In 2018, the Indian government implemented the National Cyber Security Policy, which outlines the country's objectives and strategies for cyber security, including the adoption of Cyber Security Guidelines and the establishment of the National Cyber Security Coordination Center (Neuberger, Zegart & Segal 2021a).
- The Personal Data Protection Bill was introduced in 2019 (KPMG India 2021).

These laws and regulations are intended to help protect individuals and organi-

sations from cybercrime and also to establish a legal framework for electronic commerce and digital transactions. However, the implementation and enforcement of these laws can be difficult due to existing gaps in the legal framework (Gritsenko, Wijermars & Kopotev 2021; Microsoft 2023).

## *China*

China's internet regulation began in 1993 with the Temporary Regulation for the Management of Computer Information Network International Connection. In 1994, the Regulations of the People's Republic of China for the Protection of the Safety of Computer Information Systems were passed due to the rise of computer users around the world (Qiu 2000; Endeshaw 2004). The Electronic Signature Law was passed in 2004 to regulate the use of digital signatures and protect electronic transactions (Miao, Jiang & Pang 2021). The Protection of State Secrets in Computer Information Systems on the Internet regulation is used for the monitoring of individuals' activities and potential breaches of state information The regulation also includes Internet Service Providers (I.S.P.) to monitor users' activities (Li 2015). The Regulation on Internet Information Services policy of the year 2000 controls Internet Service Providers (I.S.P.) and requires them to monitor and censor content deemed inappropriate according to government requirements (Miao, Jiang & Pang 2021). The Anti-Terrorism Law was passed in China. The law requires network operators to assist with investigations and provide access to data upon request (Wei 2020). Another key law is the Cyber Security Law (C.S.L.), passed in 2016 and came into use in 2017. The law aims to protect the country's critical information infrastructure and the personal information of citizens. These laws have been criticized by experts for being unclear giving the government too much power to control the Internet and potentially harming the interests of foreign companies (PwC 2018; Miao, Jiang & Pang 2021). The country has revised its cybersecurity laws over the years to adapt to the changing state of online crime (KPMG 2016). For example, the rise of ransomware attacks has changed the way cyberattacks are handled (Grimes 2022).

## *South Africa*

South Africa has implemented several laws and regulations to tackle cyberattacks. For example, the Electronic Communications and Transactions

Act (E.C.T.A.) of 2002. The Act provides regulations for electronic communications and transactions by organisations and end-users (Netshakhuma 2022). A National Cybersecurity Policy Framework (N.C.P.F.) was created in 2012 to help the government in its cybersecurity strategies (Phahlamohlaka, Theron & Aschmann 2022). The Protection of Personal Information (P.O.P.I.) Act was passed in 2013, for the protection of personal information. The Act commenced in 2021 to ensure organisations' compliance with the Act by indicating how end-user information will be used and data protection assurance (Veiga 2022). The 2015 Cybercrimes and Cybersecurity Bill was passed to strengthen the cybersecurity of South Africa and combat cybercrimes such as unauthorised access to computer systems (Dlamini & Mbambo 2019).

## Cybersecurity Measures Implemented in BRICS Countries

In recent years, BRICS countries have been working conscientiously, to improve their cybersecurity by implementing several policies and laws, coupled with several initiatives and establishment of organisations. The cybersecurity measures that exist among BRICS countries are discussed in the subsequent paragraphs.

### *Brazil*

Brazil has set up some agencies to implement cybersecurity measures. For example, the Brazilian Internet Steering Committee. Despite these efforts, Brazil still faces challenges such as a lack of investment in technological infrastructure and a shortage of cybersecurity professionals (Costa, Araújo, Barros, Thereza-Júnior & Costa 2022). A 2023 Information Systems Audit and Control Association (ISACA) research indicated that a lot of cybersecurity jobs remain unfilled worldwide with 81% being technical cybersecurity roles and 65% unfilled non-technical roles (ISACA 2023). In response to these challenges, the Brazilian government has launched two cybersecurity websites. The first one is a guidebook on cybersecurity and the other teaches children and young adults about cybersecurity (Urbanovics 2022). Additionally, Brazil is prioritising investing in technological critical infrastructure including the protection of information infrastructure, privacy and the personal information of its citizens (Hurel & Lobato 2021). The Brazilian government is also

partnering with private organisations to resolve cybersecurity issues. According to a study by Botacin *et al.* (2021), public and private banks in Brazil require clients to install security plugins on personal computing devices before enabling online banking use. Warsaw is an example of such a software solution. It uses a proxy server to provide online protection. In addition, the software searches for a malware pattern in a user's system.

## *Russia*

The Russian government set up the Federal Security Service (F.S.B.) as the main body responsible for cybersecurity in the country. The FSB is tasked with protecting the constitutional system, defence, and security of the state, and fighting terrorism and other serious crimes, including cybersecurity (Stadnik 2019). Additionally, specialised agencies and organisations were also established to address cybersecurity such as the National Coordination Centre for Computer Incidents (N.C.C.C.), which is responsible for protecting the country from cyberattacks (Belli 2021b). Russia also has a Federal Law on the security of critical infrastructure. This requires organisations operating critical infrastructure to ensure the security of their systems and to report certain types of cyber incidents to the government. The government also provides cybersecurity training for employees of critical infrastructure organisations (Pursiainen 2020). Despite these measures, the effectiveness of Russia's cybersecurity implementation in practice is subject to debate, as the country supposedly uses cyberattacks as a form of defence (Connell & Vogler 2016). Furthermore, the implementation of the Digital Economy National Program requires companies to store certain types of personal data within Russia's borders, which raised concerns among foreign companies, who feared that this may restrict their ability to do business in Russia and put the data at risk of being accessed by the government (Gritsenko, Wijermars & Kopotev 2021).

## *India*

To enhance cybercrime response capabilities, India set up a specific cybercrime unit in the police force, the Indian Computer Emergency Response Team (C.E.R.T.-In.) and the National Cyber Coordination Centre (N.C.C.C.) to handle computer security incidents (Belli 2021b). Skilled manpower is required. Hence, Nasscom Cyber Security Task Force (N.C.S.T.F.) was established in

India to turn the country into a cybersecurity hub by addressing issues such as the shortage of skilled cybersecurity professionals (Thakral, Rakesh & Gupta 2016). An ISACA research indicated that 52% of organisations worldwide require people to get university degrees to be offered an entry-level cybersecurity job, even though 68% of these graduates lack soft skills while 54% lack security control skills (ISACA 2023). Another challenge facing the Indian government is securing critical infrastructure from cyberattacks. The Indian government has taken several initiatives to improve the cybersecurity of critical infrastructures by establishing the National Critical Information Infrastructure Protection Centre (N.C.I.I.P.C.) to monitor and protect critical infrastructure from cyberattacks (Singh 2019).

## *China*

China has existing regulations to protect its citizens and critical infrastructure from cyberattacks. Among such are the Data Security Law (D.S.L.), Cyber Security Law (C.S.L.) and Personal Information Protection Law (P.I.P.L.). These laws assist in diverse ways to protect citizens and organisations. Furthermore, it ensures regulations and policy compliance (Chen & Sun 2021). The country also has agencies such as the Cyberspace Administration of China (C.A.C.) to implement cybersecurity measures, as well as invest in research and development of cybersecurity technologies, like artificial intelligence and quantum computing. Additionally, China has been promoting the education of cybersecurity in universities through collaborations with research institutes and other educational institutions (Chen, Wu & Liu 2020; Cary 2021).

## *South Africa*

The South African government established the Cyber Security and Cybercrime Unit of the South African Police Service to investigate cybercrimes and protect citizens from cyberattacks although the unit is not proactive (Xulu 2022). In addition, the State Security Agency (S.S.A.) was created to protect the country's national security and prevent cyberattacks (Sutherland 2017). Existing legislation to address cybersecurity includes the Protection of Personal Information (P.O.P.I.) Act, the National Cybersecurity Policy Framework (N.C.P.F.) for policy coordination, and the Cybercrimes and Cybersecurity Regulations (Romaniuk & Manjikian 2020; Dlamini & Mbambo 2019).

The BRICS association of countries have put in place diverse measures related to cybersecurity that have resulted in positive outcomes for both individuals and companies. For instance, the introduction of the National Cyber Security Policy in India; the Cyber Security Law in China; and the National Cyber Security Strategy in Russia has led to an increase in the number of cybersecurity experts in these countries, thereby enabling businesses to better defend themselves against cyberattacks. (Neuberger, Zegart & Segal 2021b; Chen & Sun 2021; Al-Qahtani & Cresci 2022). Cybersecurity is being improved in South Africa through the of use artificial intelligence for malware analysis, which enables a timely response to cyberattacks (Radebe, Tsibolane & Hart 2022). Brazil has been successful in using good cybersecurity practices to conduct incident response actions, especially during mega-events such as the Olympic games (Hurel 2021). Despite the mentioned progress, the effectiveness of cybersecurity measures among BRICS countries indicates inconsistencies.

## Discussion

BRICS association of countries are developing to become globally dominant nations through the advancement of each member's economic growth (Chen, Dao & Nhieu 2024). The rapid economic development of these nations has made member states attractive destinations for cyber threat actors to exploit. This leads to attacks on all facets of society, from governments, and private organisations to citizens. Since the advent of the internet, data breaches, identity theft, privacy invasion, cyber warfare and much more have become means of attacks (Kim, Kang, Oh, Shin & Shin; Dutta 2021). Russia and China have experienced cyber warfare with other nations and organisations due to unauthorised information access and modifications which affected the foreign relations of both countries (Elizaveta, Elnur, Kanan & Kamilla 2021). Attacks on major national infrastructure can also affect productivity and finances, which are detrimental to the economic development of BRICS countries. The impact of such cyberattacks led to the creation of policies and security measures to reduce the risks related to cyberattacks. Additionally, better cybersecurity culture needs to be adopted (Kangapi & Chindenga 2022). The existing regulations and laws make it possible to punish cyber criminals. In recent years, cyberattacks have become more sophisticated to detect, which makes it hard to penalise perpetrators (Bruce, Lusthaus, Kashyap, Phair & Varese 2024). Hence, governments, private organisations and citizens all have a part to play in the state of cybersecurity in each country.

This study indicated that policies and passive cybersecurity measures are not enough to reduce cyberattacks. Therefore, proactive measures and continuous efforts by all stakeholders are essential to attain a good level of security standards. Moreover, the financial capability of each BRICS country differs from the others and this element is important to the types and levels of cybersecurity measures implemented. Apart from establishing laws and regulations, the implementation of innovative cybersecurity measures requires financial investments from countries such as South Africa and Brazil that do not have the same financial assets as Russia and China. Poverty also plays a role in the elevation of cyberattacks in experienced in Brazil, this is indicative of the widespread banking scam in the nation. The governments of BRICS should consider improving socio-economic situations within its borders while improving current cybersecurity measures by adopting realistic best practices of other member states.

## Recommendations

### *Best Practices Adoption among BRICS Countries*

To combat cyber threats and attacks BRICS countries can share best practices. Therefore, using tested and effective cybersecurity measures. China has indicated in the past its willingness to cooperate with other countries to improve cybersecurity practices. An instance was China's expression on the issue of tackling cyberterrorism at the 68th UN General Assembly in 2014 (Wei 2020). Cooperation among BRICS countries should also be encouraged through international dialogue which may lead to the development of common cybersecurity standards and best practices. The engagement can also lead to security cooperation agreements. The Beijing BRICS Summit Beijing of 2022 was the starting point of the cooperation towards mitigating cybersecurity issues experienced by BRICS nations (Xinhua 2022).

### *More Collaborations between Government and Private Organisations*

Forging partnerships between public and private entities to combat cyberattacks is important. This strategy involves exchanging information and utilising resources, which can result in enhanced cybersecurity measures. An example was the collaborative effort between the Brazilian government and its banks.

Both entities mutually worked and established a method to reduce banking phishing attacks by adopting the use of security plugins to precede the use of banking applications (Botacin *et al.* 2021). Hence, policymakers must ensure that the cybersecurity policies are executed to achieve the intended goals rather than sabotage cybersecurity efforts (Gritsenko, Wijermars & Kopotev 2021).

### *Bridging of Cybersecurity Skill Gap*

More effort should be directed at training and recruiting cybersecurity professionals within BRICS countries. Currently, there is a global skill gap in the cybersecurity space, where many roles are left unfilled despite several government effort to train more experts in the field. Russia is making efforts towards this goal but most cybersecurity professionals relocate to developed nations such as the United States of America after attaining the required skills (Pursiainen 2020).

## Research Contribution

This study contributes to the continuous research on cybersecurity with an emphasis on government efforts in assisting to reduce the success rate of cyberattacks within each BRICS nation. The study has indicated that the government can adopt some of the best practices of other member states to provide better cybersecurity. Thus, safeguarding the society while avoiding financial loss and continuous exploitation of its citizens and organisations. These factors enable BRICS to develop into countries with better economies.

## Research Limitations and Future Works

This study highlights why the improvement of cybersecurity is important for the economic growth of BRICS countries. However, the study experienced certain limitations. The first research challenge is the number of peer-reviewed articles in scholarly journals, which are insufficient to provide current statistics on the state of cybersecurity among BRICS countries and the success rate of existing solutions. Secondly, the study would have required multinational data collection, which would have been limited by time differences and the availability of respondents if the systematic review was not used. Additionally, survey data collection would have required a longer timeframe to gather data. While telephonic interviews with experts would also depend on everyone's

availability. Future studies should consider collecting primary data from dedicated government agencies or organisations if accessible.

## Conclusion

The cybersecurity measures taken by BRICS countries are effective to varying extents. However, the adoption of best cybersecurity practices among BRICS countries is likely to help improve the state of cybersecurity. This study outlined some cyberattacks encountered in each BRICS country. These include malware, DDoS and phishing attacks which can be used to disrupt services and steal information and money. To combat these attacks, and respond appropriately, more effective cybersecurity policies and plans should be implemented. Advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML) can also provide innovative solutions to cyber threat monitoring and improve response time. Additionally, collaborations between government and private entities should be used for better implementation and enforcement of tighter cyber policies and procedures. These will enhance defences against cyberattacks which are becoming more sophisticated.

## References

Accenture 2020. Insight into the Cyberthreat Landscape in South Africa. *Accenture Insight.* https://www.accenture.com/content/dam/accenture/final/a-com-migration/manual/r3/pdf/pdf-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf

Akdemir, N. & S. Yenal 2021. How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails. *SAGE Open* 11. https://doi.org/10.1177/21582440211031879

Alieyan, K., A. Almomani, R. Abdullah, B. Almutairi & M. Alauthman 2020. Botnet and Internet of Things (IoTs): A Definition, Taxonomy, Challenges, and Future Directions. https://doi.org/10.4018/978-1-5225-9742-1.ch013

Alkhalil, Z., C. Hewage, L. Nawaf & I. Khan 2021. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer*

*Science* 3.
https://doi.org/10.3389/fcomp.2021.563060

Aslan, Ö.A. & R. Samet 2020. A Comprehensive Review on Malware Detection Approaches. *IEEE Access* 8: 6249 – 6271.
https://doi.org/10.1109/ACCESS.2019.2963724

Asuelime, L. 2018. The Pros of South Africa's Membership of BRICS: A Re-appraisal. *Journal of African Union Studies* 7: 129 - 150.
https://doi.org/10.31920/2050-4306/2018/v7n1a7

Beletskaya, M. 2022. BRICS Labor Markets: Competing with the Largest Economy. *BRICS Journal of Economics* 3,2: 75 - 96.
https://doi.org/10.3897/brics-econ.3.e85970

Bellaby, R.W. 2021. An Ethical Framework for Hacking Operations. *Ethic Theory Moral Practice* 24: 231–255.
https://doi.org/10.1007/s10677-021-10166-8

Belli, L. 2021a. Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation. *The African Journal of Information and Communication* 28: 1 - 14.
https://doi.org/10.23962/10539/32208

Belli, L. 2021b. *Cybersecurity Regulations in the BRICS Countries.* Cham, Switzerland: Springer Nature.
https://link.springer.com/book/10.1007/978-3-030-56405-6

Belli, L., W.B. Gaspar & S. Jaswant 2024. Data Sovereignty and Data Transfers as Fundamental Elements of Digital Transformation: Lessons from the BRICS Countries. *Computer Law & Security Review* 54. Special issue on Digital Transformation in the BRICS Countries.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4903196

Botacin, M., H. Aghakhani, S. Ortolani, C. Kruegel, F. Vigna, D. Oliveira, P.L. De Geus & A. Grégio 2021. One Size Does Not Fit All: A Longitudinal Analysis of Brazilian Financial Malware. *ACM Transactions on Privacy and Security* 24, 2, Article 11, 31 pages.
https://doi.org/10.1145/3429741

Bowen, G.A. 2009. Document Analysis as a Qualitative Research Method. *Qualitative Research Journal* 9,2: 27 - 40.
https://doi.org/10.3316/QRJ0902027

Bruce, M., J. Lusthaus, R. Kashyap, N. Phair & F. Varese 2024. Mapping the Global Geography of Cybercrime with the World Cybercrime Index. *PLoS ONE.* 19,4: e0297312.

https://doi.org/10.1371/journal.pone.0297312
PMid:38598553 PMCid:PMC11006133

Buarque, F., A. Gelbukh, S. Das & A. Engelbrecht (eds.). 2015. *Advances in Swarm and Computational Intelligence*. ICSI 2015. Lecture Notes in Computer Science, 9141. Cham: Springer. https://doi.org/10.1007/978-3-319-20472-7_1

Cary, D. 2021. China's Cyber AI Talent Pipeline CSET Policy Brief. *Center for Security and Emerging Technology*. https://cset.georgetown.edu/publication/chinas-cyberai-talent-pipeline/

Chahal, J., A. Bhandari & S. Behal 2019. Distributed Denial of Service Attacks: A Threat or Challenge. *New Review of Information Networking* 24: 31 - 103. https://doi.org/10.1080/13614576.2019.1611468

Checkpoint 2023. *Checkpoint 2023 Security Report*. Available at: https://go.checkpoint.com/2023-cyber-security-report/chapter-01.php (Accessed on 14 February 2023.)

Checkpoint 2024. *2024 Cyber Security Report*. Checkpoint. Available at: https://www.checkpoint.com/resources/report-3854/2024-cyber-security-report
(Accessed on 12 August 2024.)

Chen, J., J. Wu & Y. Liu 2020. Commentary on Newly Released Measures for Cyber Security Review of China. *Internaitonal Cybersecurity Law Review* 1: 87 - 91. https://doi.org/10.1365/s43439-020-00002-7

Chen, J. & J. Sun 2021. Understanding the Chinese Data Security Law. *International Cybersecurity Law Review* 2: 209 - 221. https://doi.org/10.1365/s43439-021-00038-3

Chen, Y.T., T.H. Dao & N.L. Nhieu 2024. Decoding Efficiency in Construction: A Behavioral DEA Approach to BRICS Economies. *IEEE Access* 12: 113165 - 113177. https://doi.org/10.1109/ACCESS.2024.3443925

Connell, M. & S. Vogler 2016. Russia's Approach to Cyber Warfare. CAN Analysis & Solutions. https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf

Costa, R.L., C.H.D. Araújo, V.F. de A. Barros, A.H. Thereza Júnior & L.S.O. Costa 2022. Information and Communication Technologies in the Curriculum of Basic Education in Brazil: Conceptions and Reality. SCIELO Pre-prints.

https://www.researchgate.net/publication/363241402_Information_and_Communication_Technologies_in_the_Curriculum_of_Basic_Education_in_Brazil_Conceptions_and_Reality

Dalglish, S.L., H. Khalid & S.A. McMahon 2020. Document Analysis in Health Policy Research: The READ approach. *Health Policy and Planning* 35,10, December: 1424 - 1431. https://doi.org/10.1093/heapol/czaa064 PMid:33175972 PMCid:PMC7886435

Devanny, J., L.R.F. Goldoni & B.P. Medeiros 2022. The Rise of Cyber Power in Brazil. *Revista Brasileira Política Internacional* 65,1: e013 2022. https://doi.org/10.1590/0034-7329202200113

Dlamini, S. & C. Mbambo 2019. An Exploratory Study on Mechanisms in Place to Combat Hacking in South Africa: A Criminological Perspective. *American Journal of Humanities and Social Sciences Research* 3,1: 146 - 154.

Dutta, S. 2021. Cyber Attacks on Power Grid: 10 Power Assets – Mumbai, Tamil Nadu Ports came under RedEcho Cyberattack. *India Business News – Times of India.* Available at: https://timesofindia.indiatimes.com/business/india-business/10-power-assets-mumbai-tamil-naduports-came-under-redecho-cyberattack/articleshow/81337328.cms (Accessed on 24 February 2023.)

Eldem, T. 2021. Global Cyberspace Security and Critical Information Infrastructure Protection. https://doi.org/10.1007/978-3-319-31816-5_3987-1

Elizaveta, S.S., M.T., Elnur, D.K. Kanan & D.K. Kamilla 2021. Cybersecurity Cooperation between Russia and China: Prospects and Problems. *Contemporary Chinese Political Economy and Strategic Relations: Kaohsiung* 7,3: 1319 - 1352, XII, XVII, XXI.

Endeshaw, A. 2004. Internet Regulation in China: The Never-ending Cat and Mouse Game. *Information & Communications Technology Law* 13,1: 41 - 57. https://doi.org/10.1080/1360083042000190634

Gartner 2018. The Future of Ransomware Attacks in Russia.

Gartner 2024. *Forecast Analysis: Information Security and Risk Management, Worldwide*. Gartner Research. Available at: https://www.gartner.com/en/documents/5238363 (Accessed on 19 August 2024.)

Grimes, R.A. 2022. *Detecting Ransomware, in Ransomware Protection Playbook*. Wiley.

Gritsenko, D., M. Wijermars & M. Kopotev (eds.). 2021. *The Palgrave Handbook of Digital Russia Studies.* Cham, Switzerland: Springer Nature. https://doi.org/10.1007/978-3-030-42855-6; https://link.springer.com/book/10.1007/978-3-030-42855-6

Hatcher, W., W.L. Meares & J. Heslen 2020. The Cybersecurity of Municipalities in the United States: An Exploratory Survey of Policies and Practices. *Journal of Cyber Policy* 5,2: 302 – 325. https://doi.org/10.1080/23738871.2020.1792956

Hurel, L.M., April 2021. Cybersecurity in Brazil: An Analysis of the National Strategy. A Think and Do Tank. Strategic paper 54. Igarapé Institute. https://www.researchgate.net/publication/355029919_Cybersecurity_in_Brazil_an_analysis_of_the_National_Strategy

Hurel, L.M. 2022. Interrogating the Cybersecurity Development Agenda: A Critical Reflection. *The International Spectator* 57,3: 66 – 84. https://doi.org/10.1080/03932729.2022.2095824

Hurel, L.M. & L. Lobato 2018. A Strategy for Cybersecurity Governance in Brazil. Strategic Note 30. Igarapé Institute. https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf

International Monetary Fund, October 2023. World Economic Outlook: Navigating Global Divergences. Washington, DC.

ISACA 2023. State of Cybersecurity 2023: Global Update on Workforce Efforts, Resources and Cyberoperations. ISACA.

Jiang, M. 2021. Cybersecurity Policies in China. In Belli, L. (eds.): *CyberBRICS.* Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-030-56405-6_5

Jie, Y. & L. Lin, L. 2021. Alibaba Falls Victim to Chinese Web Crawler in Large Data Leak. *The Wall Street Journal.* Available at: https://wsj.com/articles/alibaba-falls-victim-to-chinese-web-crawler-in-large- data-leak11623774850 (Accessed on 15 January 2023.)

Johnson, J., S.J. Lincke, R. Imhof & C. Lim 2014. A Comparison of International Information Security Regulations. *Interdisciplinary Journal of Information, Knowledge, and Management* 9: 89 - 116. https://doi.org/10.28945/1963

Kangapi, T.M. & E. Chindenga 2022. Towards a Cybersecurity Culture Framework for Mobile Banking in South Africa. IST-Africa Conference

(IST-Africa), Ireland 2022, pp. 1 - 8. https://doi.org/10.23919/IST-Africa56635.2022.9845633

Kim, S., J. Kang, H. Oh, D. Shin & D. Shin 2020. Operation Framework Including Cyber Warfare Execution Process and Operational Concepts. *IEEE Access* 8: 109168 - 109176. https://doi.org/10.1109/ACCESS.2020.3001286

KPMG 2016. Cybersecurity in China: A Study on National Cybersecurity Policy. *Journal of Cybersecurity* 2,2: 1 - 12.

KPMG India 2021. Cybersecurity Laws and Regulations in India: A Study of the Legal Framework. *Journal of Cyber Policy* 6,1: 45 - 58.

Kshetri, N. 2013. Cyber-victimization and Cybersecurity in China. *Communications of the ACM* 56,4: 35 - 37. https://doi.org/10.1145/2436256.2436267

Kshetri, N. 2016. Cybersecurity in Russia. https://doi.org/10.1007/978-3-319-40554-4_13

Kumar, S. & H.V. Singh 2020. Cyber Phishing: A Trap of Disguise during the COVID-19. *International Journal of Law Management and Humanities* 3,3: 1019.

Li, X. 2015. Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime. *International Journal of Cyber Criminology* 9,2.

Loureiro, M.J. & A. Loureiro & H.R. Gerber (eds.). 2022. *Handbook of Research on Global Education and the Impact of Institutional Policies on Educational Technologies*. IGI Global. https://doi.org/10.4018/978-1-7998-8193-3.ch011

Maguire, M. & B. Delahunt 2017. Doing a Thematic Analysis: A Practical, Step-by-step Guide for Learning and Teaching Scholars. *All Ireland Journal of Higher Education 9*,3. http://ojs.aishe.org/index.php/aishe-j/article/view/335.

Mallett, R., J. Hagen-Zanker, R. Slater & M. Duvendack 2012. The Benefits and Challenges of Using Systematic Reviews in International Development Research. *Journal of Development Effectiveness* 4,3: 445 - 455. https://doi.org/10.1080/19439342.2012.711342

Meyers, D. 2018. *Russian Banks Hit by Major Phishing Attacks from Two Hacker Groups*. ZDNET. Available at: https://zdnet.com/article/russian-banks-hit-by-major-phishing-attacks-from-two-hacker-groups (Accessed on 7 February 2023.)

Mi, G., Y. Gao & Y. Tan 2015. Apply Stacked Auto-Encoder to Spam Detection. In Tan, Y., Y. Shi, W. Miao, M. Jiang & Y. Pang 2021. Historicizing Internet Regulation in China: A Meta-Analysis of Chinese Internet Policies (1994 - 2017). *International Journal of Communication* 15. https://doi.org/10.1007/978-3-319-20472-7_1

Microsoft 2023. Microsoft Digital Defense Report 2023. Microsoft Threat Intelligence.

Mix, S.R. 2022. Business Continuity, Cybersecurity, and Backup Control Center: Standards, References, and Recommendations White Paper. United States: Pacific NorthWest National Laboratory. https://doi.org/10.2172/1899922

Netshakhuma, N.S. 2022. Impact of Electronic Communications and Transactions Act, No. 25 of 2002 Provision 27 in South Africa Education on Emerging Technologies. In Netshakhuma, N.S. (ed.): *Handbook of Research on Global Education and the Impact of Institutional Policies on Education Technologies.* IGI Global. https://doi.org/10.4018/978-1-7998-8193-3.ch011

Neuberger, D., A.B. Zegart & A. Segal 2021a. Cybersecurity in India: A Study on National Cybersecurity Policy. *Journal of Cybersecurity* 7,1: 1 - 12.

Neuberger, A., A.B. Zegart & A. Segal 2021b. The Cybersecurity Threat from Russia. Conference of the Digital and Cyberspace Policy Program. [Symposium]. U.S.A.

Oppermann, D. 2014. Internet Governance and Cybersecurity in Brazil. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2587178

Page, M.J., J.E. McKenzie, P.M. Bossuyt, I. Boutron, T.C. Hoffmann, C.D. Mulrow, L. Shamseer, J.M. Tetzlaff, E.A. Akl, S.E. Brennan, R. Chou, J. Glanville, J.M. Grimshaw, A. Hróbjartsson, M.M. Lalu, T. Li, E.W. Loder, E. Mayo-Wilson, S. McDonald, L.A. McGuinness & D. Moher 2021. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ (Clinical Research Education)* 372, n71. https://doi.org/10.1136/bmj.n71 PMid:33782057 PMCid:PMC8005924

Pieterse, H. 2021. The Cyber Threat Landscape in South Africa: A 10-Year Review. *The African Journal of Information and Communication* 28: 1 - 21. https://doi.org/10.23962/10539/32213

Phahlamohlaka, J., J. Theron & M.J. Aschmann 2022. National Cybersecurity Implementation in South Africa: The Conundrum Question. *Journal of Information Warfare* 21,1: 1 - 16.

Pursiainen, C. 2020. Russia's Critical Infrastructure Policy: What Do We Know About it? *European Journal for Security Research* 6:21 - 38. https://doi.org/10.1007/s41125-020-00070-0

PwC 2018. Cybersecurity in China: A Study on National Cybersecurity Policy. *Journal of Cybersecurity* 4,1: 1-12.

Qiu, J.L. 2000. Virtual Censorship in China: Keeping the Gate Between the Cyberspaces. *International Journal of Communications Law and Policy* 4: 1 - 25. https://ciaotest.cc.columbia.edu/olj/ijclp/ijclp_4/ijclp_4a.pdf

Radebe, M., P. Tsibolane & M. Hart 2022. Perceptions of AI Tools for Cybersecurity in Large Enterprises. ICDSST 2022 Proceedings. The EWG-DSS 2022 International Conference Decision Support System Technology.

Rawindaran, N., A. Jayal, E. Prakash & C. Hewage 2021. Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME). *Future Internet* 13,8: 186. MDPI AG. Available at: https://doi.org/10.3390/fi13080186 (Accessed on 3 February 2023.)

Republic of China 2022. XIV BRICS Summit Beijing Declaration. The Republic of China. https://bricsthinktankscouncil.org/wp-content/uploads/2022/06/14th-BRICS-Summit-Beijing-Declaration.pdf

Romaniuk, S. & M. Manjikian 2020. *Routledge Companion to Global Cyber-Security Strategy*. London & New York: Routledge. https://doi.org/10.4324/9780429399718

Romagna, M. 2020. Hacktivism: Conceptualization, Techniques, and Historical View. In Holt, T. & A. Bossler (eds): *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3_34

RSA Research Group 2014. *RSA Discovers Massive Boleto Fraud Ring in Brazil*. RSA Research Group.

Saleous, H., M. Ismail, S.H. AlDaajeh, N. Madathil, S. Alrabaee, K.R. Choo & N. Al-Qirim 2023. COVID-19 Pandemic and the Cyberthreat Landscape: Research Challenges and Opportunities. *Digital Communications and Networks* 9,1: 211 – 222. https://doi.org/10.1016/j.dcan.2022.06.005

SARS 2022. *Scams and Phishing.* South African Revenue Service. Available at: https://sars.gov.za/targeting-tax-crime/scams-and-phishing

(Accessed on 7 February 2023.)

Sethi, A. 2020. The Indian Information Technology Act: A Study of its Impact on Cybercrime. *Journal of Cyber Policy* 5,2: 87 - 99.

Shukla, M., S.D. Johnson & P. Jones 2019. Does the NIS Implementation Strategy Effectively Address Cyber Security Risks in the UK? 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK. https://doi.org/10.1109/CyberSecPODS.2019.8884963

Shulzhenko, N. & S. Romashkin 2020. Internet Fraud and Transnational Organized Crime. *Tribuna Juridică* 21: 162-172.

Shvets, P. 2020. Cybersecurity in Russia: A Study on National Cybersecurity Strategy. *Journal of Cybersecurity* 6,1: 1 - 12.

Singer, P.W. & A. Friedman 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford, New York: Oxford university Press.

Singh, S. 2019. India's National Cyber Security Policy: Gaps and the Way Forward. (SSPC Monograph Series No. 2.) New Delhi: Jawaharlal Nehru University, Society for the Study of Peace and Conflict. https://doi.org/10.13140/RG.2.2.35459.63524; https://doi.org/10.1093/wentk/9780199918096.001.0001

Stadnik, I. 2019. Sovereign Runet: What Does it Mean? Internet Governance Project. https://www.internetgovernance.org/research/sovereign-runet-what-does-it-mean/

Sutherland, E. 2017. Governance of Cybersecurity – The Case of South Africa. *The African Journal of Information and Communication (AJIC)* 20: 83 - 112.

Thakral, A., R. Rakesh & A. Gupta 2016. 'Space in Space': Cyber Security Capabilities in Indian Context. 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, India 2016, pp. 1 - 6. https://doi.org/10.1109/GET.2016.7916715

Tie, C.Y, M. Birks & K. Francis 2019. Grounded Theory Research: A Design Framework for Novice Researchers. *SAGE Open Medicine* 7. https://doi.org/10.1177/2050312118822927

UNDP 2022. *Cybersecurity in BRICS Nations*. Available at: https://undp.org/content/undp/en/home/sustainable-development-goals/goal-16-peace-justice-andstrong-institutions/cybersecurity-in-brics-nations.html

(Accessed on 11 February 2023.)
https://doi.org/10.1177/2050312118822927
PMid:30637106 PMCid:PMC6318722

Urbanovics, A. 2022. Cybersecurity Policy-Related Developments in Latin America. *AARMS* 21,1: 79 - 94.
https://doi.org/10.32565/aarms.2022.1.6
https://www.internetgovernance.org/research/sovereign-runet-what-does-it-mean/

Van Niekerk, B. 2017. An Analysis of Cyber-incidents in South Africa. *The African Journal of Information and Communication (AJIC)* 20: 113 - 132.
https://scielo.org.za/pdf/ajic/v20/06.pdf

Vaz Ferreira, L. 2022. Cybersecurity and Ransomware in the Brazilian Government. *Revista InterAção* 13,1: 58 - 65.
https://doi.org/10.5902/2357797570703

Veiga, A. 2022. A Study on Information Privacy Concerns and Expectations of Demographic Groups in South Africa. *Computer Law & Security Review* 47.
https://doi.org/10.1016/j.clsr.2022.105769

Wei, X. 2020. A Critical Evaluation of China's Legal Responses to Cyberterrorism. *Computer Law & Security Review* 47: 105768.
https://doi.org/10.1016/j.clsr.2022.105768

World Economic Forum 2020. *Cybersecurity in BRICS Nations*. Available at: https://weforum.org/agenda/2020/03/cybersecurity-in-brics-nations (Accessed on 7 January 2023.)

World Economic Forum 2021. *The Cost of Cybercrime*. Available at: https://weforum.org/agenda/2021/03/cost-of-cybercrime-2021-report (Accessed on 2 January 2023.)

Xinhua 2022. BRICS Countries Committed to Creating a Unified Solution to Cybercrime.

Xulu, H. 2022. *The New Private Security: Regulating Cybersecurity Services in South Africa*. Private Security Industry Regulatory Authority.

Zieni, R., L. Massari & M.C. Calzarossa 2023. Phishing or Not Phishing? A Survey on the Detection of Phishing Websites. *IEEE Access* 11: 18499 - 18519.
https://doi.org/1109/ACCESS.2023.3247135

Zdziarski, J. 2018. The Russian Government and Cybercrime: A Study of Laws and Regulations. *Journal of Cyber Policy* 3,1: 23 - 35.

*A Survey of Cybersecurity Issues in BRICS Countries*

Oluwafisayo Kaka
Cybersecurity & AI Business Services
Software Carpentry Workshops Practitioner
oluwafisayo.kaka@gmail.com

# Chapter 9: Fostering Good Governance and Human Rights in an Expanded BRICS: Challenges and Opportunities

**Simbarashe Tembo**
**ORCID iD: https://orcid.org/0000-0001-7491-6765**

**James Ndlovu**
**ORCID iD: https://orcid.org/0009-0004-2945-031X**

## Abstract

The expansion of the BRICS adds to the diversity of economic and political systems amongst its members. With new and existing membership, ranging from liberal constitutional democracies to outright authoritarian regimes, the BRICS bloc will face a myriad of challenges in policy formulation and implementation. While diversity is often desirable, it is crucial for the bloc to establish normative principles for good governance, democracy and human rights and foster mutual respect and shared values among member states. It is argued in this paper that as BRICS positions itself as an alternative to Western-led global institutions, a principle-based approach to its relations can bolster its moral authority in international affairs. A significant number of countries that have recently joined BRICS face significant challenges including repression, corruption and political and economic instability. This paper theorizes that a shared commitment to human rights and good governance enhances economic development, peace and security leading to more equitable and inclusive growth in member states. Relying on liberal theories of international relations and international law, the paper will firstly discuss the imperative for setting international human rights norms, tailored context specific for BRICS countries, in enhancing cooperation within the bloc. The paper will then attempt to provide technical assistance by drawing from best practices to facilitate human rights-based cooperation and among member states. It will be shown that an expanded BRICS has potential to reinforce good governance, human rights and democracy.

**Keywords**: Good governance, human rights, BRICS+, liberal institutionalism, democratic peace theory

## Introduction and Background

At its inception in 2009, BRICS was made up of four countries, that is Brazil Russia, India, and China. South Africa joined the group at the 2011 Summit in China. Since then, BRICS has been a force to reckon within global affairs as it represents the world's biggest emerging markets. BRICS therefore remains 'a core of south-south cooperation, promoting the interests of a group of developing countries in global governance for a more balanced global architecture' (Kirton & Larionova 2022:8). After the joining of South Africa in 2011, BRICS became a 'transregional governance mechanism with a comprehensive political, security, economic and social agenda' (Kirton & Larionova 2022). BRICS is a diverse group with marked differences in the sizes of the members' economies, governance systems, and cultures (Lipton 2017). This diversity poses a significant challenge to the harmonization of policies particularly in the area of human rights. Scholars have always seen its ideological and political heterogeneity as posing a risk to the capability to achieve its objective of establishing a collective world order. History has shown that due to its diversity, BRICS has failed to craft a cohesive foreign policy, especially on the Libyan issue in 2011 when national and diplomatic interests took priority over a common position (Gilbert 2019). Daniel and Virk (2014: 21) observe that 'South Africa voted for UN Security Council Resolution 1973, authorising Anglo-French-led intervention in Libya, while Brazil, Russia, India, and China all abstained'. So far, the BRICS, has only registered cohesion in its anti-West stance. The expansion of BRICS on 1 January 2024 to include five more countries has made it even more diverse. At its 15th Summit in Johannesburg in August 2023, BRICS invited six more countries to join its ranks (Argentina, Egypt, Ethiopia, Iran, Saudi Arabia and the United Arab Emirates). Argentina subsequently declined (Steenhagen 2024). On the global affairs front, commentators have posited that the heterogeneity of the BRICS is likely going to limit the group's influence in world trade and the international monetary system (Afota *et al.* 2024). It has been argued that:

> At this stage, the expansion mainly serves to underline the alliance's attractiveness for emerging and developing countries, which see it as a

> forum for expression for the 'Global South', and helps to establish the enlarged bloc (BRICS+) as a major force in global economic governance (Afota *et al.* 2024).

The expansion of BRICS has essentially shifted its goal from just strengthening the voices of emerging economies and participation in international affairs towards 'global politics and strengthening alliances to combat Western imperialism and dominance, focusing on the right to development' (Fairplanet 2023). This article posits that the expansion of BRICS and its involvement in global affairs is a welcome development, however, the bloc also needs to focus on the issues of rule of law, democracy, and human rights, or else it will devolve into a dictators' club. Critics of the expanded BRICS have already labeled it an 'international repressive alliance' (CIVICUS 2023). Justification for this lies in China and Russia's human rights record. The United Nations Human Office of the High Commissioner for Human Rights (2022) has previously reported that there are possible crimes against humanity committed by China in Xinjiang region where religious minorities, Uyghurs, and Kazakhs suffer arbitrary detentions, arrests, and torture. The International Criminal Court also has a pending warrant of arrest for Russia's President, Vladimir Putin, for committing war crimes in Ukraine. Amnesty International implored South Africa's President Cyril Ramaphosa to speak against atrocities that were being committed by Russia:

> President Ramaphosa cannot say BRICS wants to contribute to a better world when South Africa is silent on human rights atrocities being perpetrated by its members. The Russian government is not only violating international humanitarian and human rights law in its war of aggression against Ukraine, but its crackdown on people in Russia who are speaking out about the invasion goes against the rights to freedom of expression and assembly which South Africa and its Constitution prides itself on (Amnesty International 2022).

It is also reported that the human rights situation in India has deteriorated, and South Africa's socio-economic landscape remains largely unequal. The newcomers' human rights record also paints a bleak picture- war crimes in Ethiopia and wanton violation of religious minority rights in Saudi Arabia. CIVICUS Monitor reports that the civic space in 6 of the 11 BRICS+ countries is shut down. The 15$^{th}$ BRICS SUMMIT Declaration adopted at the August

2023 Summit in Johannesburg expressed the members' commitment to 'enhancing and improving global governance by promoting a more agile, effective, efficient, representative, democratic and accountable international and multilateral system' (BRICS 2023: 2). More expressly, the Member states affirmed their commitment to 'ensuring the promotion and protection of democracy, human rights and fundamental freedoms for all with the aim to build a brighter shared future for the international community based on mutually beneficial cooperation' (BRICS 2023: 2). This article avers that for the commitments to be achieved, the BRICS+ group will need to first align member states' legal and ideological perspectives to avoid a discordant approach. While writing for Business Day, Mia Swart notes that:

> While few countries have squeaky clean human rights records, the scale and extent of human rights violations in China, Russia and India are staggering. Whatever membership criteria get decided on they are sure not to include human rights, democracy or the rule of law, since if compliance were to become a criterion, most of the current BRICS members would have to be suspended (*Business Day* August 2023).

While the BRICS+ makes commitments to human rights, pessimists argue that these countries' human rights track records render these commitments palpably insincere. An argument has been made that the leaders of the majority of BRICS+ countries cannot promote democratic governance of international institutions, while they do not support democracy at home. This significantly blights the BRICS+ group's commitment to its values and assertions.

## Theoretical Framework

This paper examines the intricate relationship between the expansion of BRICS, the promotion of good governance, and the protection of human rights. To this end, the paper draws upon liberal theories of international relations and international law, particularly liberal institutionalism and democratic peace theory.

### *i) Liberal Institutionalism*

Liberal institutionalism posits that international institutions can play a pivotal role in fostering cooperation among states, even in the face of divergent interests (Acharya & Buzan 2019; Keohane & Martin 1995; Keohane 2005). By examining BRICS+ through the lens of liberal institutionalism, the paper seeks

to investigate how the bloc can establish norms, facilitate cooperation, and potentially create mechanisms for monitoring and encouraging compliance with human rights and good governance standards among its members. The tenets of liberal institutionalism suggest that clear norms, effective monitoring mechanisms, and opportunities for dialogue are crucial for successful cooperation within international institutions (Ruggie 1993; Hale & Held 2017). As such, this study utilizes these tenets to assess the effectiveness of different institutional designs within BRICS for achieving its human rights and good governance goals. It also explores factors that might promote or hinder cooperation within BRICS on these issues, such as power dynamics, the level of institutionalization, and the presence of shared interests.

### *ii) Democratic Peace Theory*

Democratic peace theory suggests that democratic states are less likely to engage in conflict with each other and tend to uphold better human rights records (Russet 1993; Gartzke 2007; Mousseau 2013; Hellmann 2020). While not all BRICS members are democracies, the theory remains relevant due to the increasing diversity of political systems within the group. The presence of democratic states like South Africa, Brazil, and India alongside less democratic ones creates a dynamic that can be analyzed to understand the potential for BRICS+ to promote human rights and good governance. The theory is crucial in exploring two key aspects of BRICS+,

(i) the potential influence of democratic members on the BRICS agenda, particularly in advocating for human rights and good governance; and

(ii) the potential for BRICS+ to become a platform for promoting democratic values and practices, even among non-democratic members, thus contributing to a gradual shift towards greater respect for human rights and good governance across the bloc.

## Methodology

This study adopts a qualitative research design. It relies on secondary data in the form of published and unpublished literature sources on the study phenomenon. The study delves into the complexities of the BRICS+ bloc, particularly in the area of governance and human rights. To succinctly explain

the disjuncture between members' human rights posture, a comparative analysis is adopted. In so doing, the study makes reference to South Africa, Russia, China, Brazil, Iran, and Saudi Arabia, among others. This allows for an in-depth exploration of the human rights discord within the bloc within a real-world context. This has facilitated a nuanced understanding of the interplay between individual countries' human rights agenda and the bloc's indifferent approach.

## The Evolution of the BRICS

At its inception in 2009, the BRIC, was characterized and defined by the economic power that the four nations of Brazil, Russia, India and China wielded as the major emerging markets. These four nations sought to challenge the post-Cold War trends that were characterized by inequality, polarization, hegemonic and discriminatory world order (Patnaik 2022). The group was dedicated to the interests and cooperation of its member states to enhance global governance. It morphed into a major international organization with annual summits to develop and implement its policies and interests. According to Rivers (2015: 578), 'the cooperation of these states in formalized summits has proven to be beneficial in the promotion of common interests and objectives'. One such example is that the 2014 summit culminated in the BRICS New Development Bank with the purpose of 'mobilizing resources for infrastructure and sustainable development projects in BRICS and other emerging developing economies' (Rivers 2015: 578). The New Development Bank (NDB) was created as an alternative to the dominant Bretton Woods institutions such as the World Bank and the International Monetary Fund (IMF) (Dixon 2015). The main focus of the NDB was to fund infrastructure and sustainable development projects in BRICS and other developing countries. In addition to the NDB, BRICS also established the Contingent Reserve Agreement (CRA), a framework that enables the provision of liquidity support to members in case of financial difficulty. What is strikingly different between the BRICS institution and other Western-led institutions is that of political identity. Western-led institutions' members' identities converge on the ideals of liberal democracy while BRICS membership has no political identity. Their only mutual identity is that of being developing countries or emerging markets. As such, this lack of political identity casts a huge shadow on the group's prospects of success. Rivers (2015: 578) notes that 'questions regarding the capability of five countries with fundamentally different political identities to merge into what appears to be an increasingly important political group have developed'.

## BRICS+ Members and Human Rights

China is considered the most significant actor within the BRICS+ (Beeson & Zeng 2018). China continues to adhere to its policy of non-intervention in its engagements with other states. China's non-intervention policy means that it is willing to engage in business with any state without being involved in the internal affairs of that particular country. Such a stance has received significant criticism as it demonstrates China's willingness to conduct business with even rogue states/ regimes complicit in human rights abuses (Mumuni 2017). China maintains that national governments should focus on and respond to domestic socio-political and/or economic issues. This adherence to the policy of non-intervention has crippled Beijing's ability to engage in international interventions meaningfully. However, this article argues that advancing a non-interventionist stance in the face of human rights violations can be detrimental to international peace and good governance.

Unlike China which has formulated and maintained the policy of non-intervention in which it is reluctant to intervene in the affairs of other nations, Russia on the other hand has a much more aggressive stance. Russia's approach to human rights is largely influenced by its more authoritarian political structure, internally. Autocrats' behaviour at the international level reflects their governing methods at home, where, in the absence of a genuine popular mandate, they rely on a crude combination of corruption and force to maintain control (Freedom House 2023). Russia's aggressive foreign policy is characterized by violations of international law and the principle of sovereignty, as seen by its full-scale invasion of Ukraine in a bid to scuttle that country's hard-won democratic progress. Russia's approach largely resists any external critics of its internal and foreign engagements.

The political systems of the BRICS+ nations are different from each other. The majority of the member states have been characterised as undemocratic. China, Russia, Saudi Arabia, UAE, Iran have been characterised as outrightly authoritarian regimes while Egypt and Ethiopia are more inclined to authoritarianism than democracy, and India demonstrates fascist tendencies under the current regime (Ullah *et al.* 2024). This is quite alarming as only two out of ten nations are considered democratic. The implication is that most of the BRICS nations are authoritarian regimes with no space for civil societies. Such an environment is characterised by gross human rights violations. As Annor (2023:1) argues, 'we do see a group of countries that certainly have a democracy problem, and this is strengthening non-democratic trends in the BRICS, and a

human rights problem'.

Essentially, only two members, South Africa and Brazil are faced with the mammoth task of advocating for human rights and democracy within BRICS+. This is a huge task considering that decisions within BRICS are made by consensus. Therefore, it is likely to be difficult to charter a democratic course within BRICS that is based on respect for human rights and dignity.

## Human Rights Abuses and Repressive Regimes

Russia's perspective on human rights is heavily influenced by its focus on state sovereignty and non-intervention. Russia often views human rights through the lens of protecting national sovereignty and resisting external pressures, particularly from Western countries. Such a perspective can sometimes lead to resistance against international human rights norms perceived as infringing on state sovereignty (Staniste 2015).

Recent reports of human rights violations in Russia have painted a gloomy image of the country's human rights situation. For instance, there has been reported crackdown on civil society, systematic persecution of human rights defenders, and widespread restrictions on freedom of expression. In April 2022, Russian authorities revoked the registration of 15 foreign NGOs and foundations, forcing them to shut their offices in Russia, including Human Rights Watch and Amnesty International (Human Rights Watch 2023). While this crackdown on civil society groups received international scrutiny and widespread condemnation, the BRICS partners turned a blind eye. Russia's human rights record has faced significant international scrutiny in recent years. The government has enacted a series of restrictive laws that severely limit freedom of expression, assembly, and association. Independent media outlets and civil society organizations critical of the government have faced increasing pressure, including closures, harassment, and criminal prosecutions.

The crackdown on political opposition has intensified, with prominent figures like Alexei Navalny facing imprisonment and targeted attacks (Amnesty International 2023b). The arbitrary detention and prosecution of peaceful protesters demonstrate a disregard for basic civil liberties. The ongoing conflict in Ukraine has further exacerbated concerns about human rights abuses, with reports of war crimes and violations of international humanitarian law.

China's approach to human rights in BRICS is heavily shaped by its one-party system, which prioritizes state control and stability over individual freedoms. China often promotes a narrative which emphasizes economic and

social rights over political rights. This perspective aligns with its broader international strategy of resisting Western-dominated human rights discourses (Boer 2020). The Chinese government promotes a vision of human rights that prioritizes economic development and social stability, often framing these as prerequisites for the enjoyment of individual rights (Subedi 2015).

However, reports indicate that Chinese authorities continue to suppress opposition and any dissenting voices, it continues to restrict media freedom, and there continues to be widespread persecution of human rights defenders. According to the Freedom House Report, the Communist Party regime in China has remained one of the world's worst abusers of political rights and civil liberties, and those who criticise the party receive severe penalties (Freedom House 2015). Authorities continue to harass, detain, and persecute human rights defenders. For example, a human rights lawyer, Tang Jitian, was forcibly disappeared by authorities in Jilin Province in December 2021. Authorities had previously stopped him from leaving the country to visit his daughter, who was getting medical treatment in Japan (Human Rights Watch 2023). The authorities also continue to curtail freedom of expression as reports of people being harassed, detained, and prosecuted for their online posts and private chat messages critical of the government are common. For instance, in May 2022, a court in Hainan province sentenced former journalist Luo Changping to seven months in prison for a Weibo post that questioned China's justification for its involvement in the Korean War (Human Rights Watch 2023). This highlights a situation where those in power are violating human rights without impunity. As a result, Freedom House has ranked China near the absolute bottom in terms of overall political rights and civil liberties (Freedom House 2023). This presents a challenge to the BRICS bloc in seeking to advance a human rights agenda.

India's perspective on human rights is influenced by its democratic values. According to Varela & Delgado (2019) within BRICS, India supports human rights but with a strong emphasis on development and poverty alleviation, sometimes leading to a prioritization of economic growth over strict human rights standards. India's stance on human rights emphasises economic growth and alleviating poverty as fundamental pillars to improving human rights. India has a considerably strong commitment to upholding democratic principles and fundamental freedoms. India also shares concerns about external interference in its domestic affairs, often advocating for a balanced approach that respects sovereignty while promoting development (Hieronymi & Karimov 2023). However, India's own challenges with human rights, including concerns about restrictions on freedom of expression, discrimination against minorities,

and the situation in Kashmir, raise questions about its ability to champion human rights within BRICS consistently and the international community at large. Democratic rights in India remain under pressure, particularly for marginalised groups, with authorities in Uttar Pradesh responding to Muslim-led protests by demolishing the property of Muslim citizens (Freedom House 2023).

Brazil generally takes a more progressive stance on human rights rooted in its democratic framework. Brazil's participation in BRICS reflects a balance between promoting human rights and engaging in South-South cooperation that sometimes prioritizes economic development over strict adherence to human rights standards (Pomeroy *et al.* 2016).

The newly added members of the BRICS+ bloc have also added to the discord. These countries are also grappling with human rights issues in their countries. Ethiopia is ranked amongst the Not Free category as it lacks many aspects of the rule of law that might protect its citizens' fundamental human rights (Freedom House 2023). This worst ranking is mostly attributed to the ongoing civil conflict centred on the northern Tigray region, which has resulted in, among other abuses, extrajudicial killings, enforced disappearances, and the expulsion of hundreds of thousands of people from their homes based on their ethnicity.

The latest inclusion of Iran in the expanded sparked controversy as Iran is largely considered to be the world's largest state sponsor of terrorism is currently engaged in a number of regional conflicts via its proxies and a decade long war against fellow BRICS member and regional rival Saudi Arabia in the Yemen (Ross 2024). On the domestic scene, Iran has had a fair of human rights violations which have tainted its international human rights record. A case in point would be its removal from the UN Commission on the Status of Women and prevention from serving the rest of its four-year term as a result of a resolution introduced by the United States and supported by 28 other countries (Freedom House 2023). This removal was in response to the Iranian government's campaign to suppress the rights of women and girls by using force against protesters which in essence undermined the UN's mission to promote gender equality. The question then arises as to how Iran can be able to advance the progressive promotion of human rights within BRICS, given such a tainted history. This raises the need for a human rights framework within BRICS which will lead to the adherence to human rights principles by all member states.

Similarly, Saudi Arabia has also attracted criticism for its poor human rights record and extrajudicial killings (Ross 2024). There are widespread

reports of human rights abuses in Saudi Arabia which further tarnishes the image of BRICS. A case in point would be how ordinary people are less free to express their views to others, whether online or offline, due to restricted freedom of expression. For example:

> In August 2022, a terrorism court in Saudi Arabia sentenced Nourah bint Saeed al-Qahtani to 45 years in prison merely for social media posts, just weeks after handing a 34-year sentence to another woman, Salma al-Shehab, for sharing posts by a Saudi dissident (Freedom House 2023).

It is difficult to understand how a repressive government like that of Saudi Arabia can be associated with the other more democratic governments within the BRICS.

## Lack of a Coherent Human Rights and Governance Position within BRICS

It is evident that BRICS+ does not have a coherent joint position on human rights and good governance. This is not surprising given the nature of the bloc which has mostly sought to provide an alternative order. There seems to be convergence on the economic front and a discord on the political and human rights front. This is discord presents a major stumbling bloc to future collaboration and cooperation of BRICS nations especially on the promotion of human rights and good governance. It has been argued that while there has been increased cooperation and interaction within the expanded BRICS+, the avenues for future cooperation are limited by fundamental differences among the BRICS+ states (Glosny 2010). Thus far there has not been any significant initiative or advancement that has prioritised issues of human rights and the member states of the BRICS+ club have tip-toed on the issues when any of their members have been confronted with allegations of human rights violations.

A look at the responses and actions by the BRICS nations in response to the Russia/Ukraine conflict is evidence of this discord and the lack of appetite by the member states to stand against human rights violations. For instance, Brazil sent mixed messages as the Brazilian administration concerning the war in Ukraine was not inconsistent. According to the Human Rights Watch Report:

> A few days before Russia's full-scale invasion, then President Bolso-

> naro said, in Moscow, that Brazil stood 'in solidarity with Russia'. Over the following months, Brazil voted for a UN resolution establishing a commission to investigate war crimes in Ukraine but abstained on one suspending Russia's membership on the UN Human Rights Council and opposed a World Trade Organization declaration on the war's devastating impact on Ukraine's ability to export and import (Human Rights Watch 2023).

On the other hand, India also abstained during votes on resolutions at the United Nations related to Russia's invasion of Ukraine, including a UN General Assembly resolution adopted in March censuring Russia for its military actions and calling on Moscow to withdraw its troops unconditionally (Human Rights Watch 2023). Similarly, South Africa, though a human rights defender, globally, it also maintained a neutral stance choosing instead to abstain from a UNGA vote to suspend Russia from the UN Human Rights Council. Therefore, the BRICS nations need a human rights framework with a shared commitment to human rights and good governance to enhance economic development, peace, and security, leading to more equitable and inclusive growth in member states. Regrettably, South Africa, with its human rights reputation, has never adopted an agenda to influence fellow BRICS countries' human rights.

## Opportunity for Corporation and Knowledge Sharing

Despite the numerous challenges facing the BRICS+, the bloc boasts of significant opportunities to bolster cooperation and the sharing of knowledge amongst the member states. The knowledge sharing can be in the form of shared best practices between the members. For instance, countries with a record of good governance and human rights promotion within the bloc, such as South Africa and Brazil, can be at the forefront of championing these values and practices that are advanced by all member states in the bloc. Liberal institutionalism emphasizes the potential for international institutions to foster cooperation and peace. Therefore, within BRICS+, South Africa and Brazil, with their democratic institutions, can play a crucial role in promoting transparency, accountability, and good governance. This aligns with Democratic Peace Theory, which suggests that democracies are less likely to engage in conflict with each other. Thus, these nations could spearhead peaceful and cooperative engagements, enhancing the overall functionality of BRICS+ (Stojković & Milosavljević 2023). Their roles in fostering cooperation in

economic development and governance could pave the way for addressing human rights concerns within the bloc, potentially leading to future collaborations on governance and democratic reforms (Nuruzzaman 2020). Establishing a balance between economic development and the preservation of democratic principles within the BRICS+ framework as it evolves as a major global institution is necessary. By leveraging their democratic frameworks, South Africa and Brazil can advocate for better governance and civil liberties within BRICS, enhancing their position as a global leader in both economic and human rights matters (Duggan *et al.* 2021).

## Building a Human Rights Agenda within the BRICS+

While the political systems within BRICS+ differ significantly, there is potential to build a human rights agenda by focusing on economic and social rights, which is prioritised by some states within the bloc. The liberal institutionalism perspective suggests that cooperation through international institutions fosters peace and prosperity, and BRICS+ could adopt this approach by prioritising economic development as a foundation for advancing the human rights agenda. India's long-standing focus on development and poverty alleviation aligns its human rights agenda with broader international standards by emphasizing economic and social rights, which are crucial for alleviating poverty and improving livelihoods. This approach aligns with the Sustainable Development Goals (SDGs), particularly SDG 1 (No Poverty), and reflects the liberal institutionalist idea that states can cooperate to achieve mutual benefits, even with differing political systems (Vyas-Doorgapersad 2021). Building a shared framework for human rights within BRICS+ could strengthen the bloc's ability to address violations against human rights and advance the promotion of civil liberties. A human rights framework could be rooted in shared economic interests, incentivizing member states to adhere to human rights principles as a means to bolster economic growth and cooperation (Singh 2019).

As a new member in the bloc, Saudi Arabia, for example, has faced significant criticism for its poor human rights record, including restrictions on freedom of expression and reports of extrajudicial killings. Addressing these issues within the BRICS+ framework presents a challenge, as some members prioritize sovereignty and non-interference. However, the bloc can promote gradual improvement in these areas by integrating human rights into BRICS+ economic and development agendas. As such, the member states could thus benefit from aligning with the economic growth and governance reforms

advocated by BRICS+, which emphasize development as a pathway to improved human rights. The shared focus on economic development has the potential to create a platform for BRICS+ to integrate governance reforms that address human rights issues, making development and human rights complementary goals (Panova 2021). Developing such a framework would require overcoming the bloc's political heterogeneity, but focusing on economic cooperation and governance reforms could pave the way for addressing broader human rights concerns. As BRICS+ continues to grow and diversify, it has the potential to evolve into a platform where all member states (whether democratic or non-democratic) can find common ground on issues such as human rights, without sacrificing their sovereignty or economic interests. The establishment of governance frameworks that integrate human rights into economic policies would reinforce the role of BRICS+ as a global leader in promoting sustainable and equitable development (Duggan *et al.* 2021).

## Expanding Civic Space and Civil Society Engagement

Expanding civic space and engaging civil society within BRICS+ presents a crucial opportunity for enhancing good governance and promoting human rights. As BRICS+, evolves and transforms into a formidable institution, it has a unique opportunity to integrate civil society into governance structures. The liberal institutionalist perspective emphasizes cooperation through international institutions and recognizes the vital role of non-state actors, such as civil society organizations (CSOs), in policymaking processes. Hence, including civil society can foster greater accountability, transparency, and public participation, which are critical for improving good governance within the BRICS+ bloc. Studies have indicated that democratic civic institutions in countries with higher levels of socio-economic development exhibit greater political activity and effecttiveness in holding governments accountable (Gryshchenko *et al.* 2021). While many BRICS+ members, particularly the less democratic states, restrict civil liberties, the democratic countries within the bloc, are well-positioned to lead efforts to promote civic engagement and expand the space for civil discourse. This suggests that the democratic members of BRICS+ can effectively advocate for including civil society in decision-making processes, thus promoting governance reforms that align with democratic principles (Papa, Han & Anon 2023).

Promoting civic engagement and expanding space for civil discourse could help BRICS+ develop a more inclusive human rights agenda. Civil

society organizations, particularly in South Africa and Brazil, have been effective in advocating for human rights and good governance. Their participation in BRICS+ processes can help address systemic human rights concerns across the bloc. By involving these organizations, BRICS+ can harness the strength of democratic governance to ensure that civil society plays a vital role in policy formulation and implementation. This is essential for building trust and legitimacy in governance, particularly in a politically diverse bloc like BRICS+ (Duggan, Ladines Azalia & Rewizorski 2021). This expansion of the civic space in BRICS+ aligns with the goals of liberal institutionalism, which emphasizes the importance of including diverse stakeholders in international governance processes. Institutions that integrate civil society are better positioned to respond to complex global challenges, such as human rights violations and bad governance. These organisations are crucial in advocating for marginalized groups, holding governments accountable, and contributing to good governance (Scholte 2020).

## Conclusion

BRICS member states have diverse political systems and human rights records. Reaching a consensus on human rights standards and implementation could be challenging. Some BRICS+ members have been criticised for restricting civil and political liberties. There are concerns that the bloc could prioritise state sovereignty and economic development over individual rights and freedoms. This discord amongst the BRICS+ member states pose a serious threat to its very own existence. There is a need for the bloc to develop a framework for human rights and demonstrate a shared commitment towards protection of the rights of the people.

## References

Acharya, A. & A. Buzan 2019. *The Making of Global International Relations.* Cambridge University Press. https://doi.org/10.1017/9781108647670

Afota, A., V. Burban, P. Diev, F. Grieco, T. Iberrakene, K. Ishii, M. Lopez-Ferero, Q Paul, F. Sammeth, C. Valadier 2024. Expansion of BRICS: What are the Potential Consequences for the Global Economy? Banque de France Bulletin February 2024. Available at: https://www.banque-

france.fr/en/publications-and-statistics/publications/expansion-brics-what-are-potential-consequences-global-economy (Accessed on 27 June 2024.)

Amnesty International 2022. Press Statement, 22 June 2022. South Africa/ China: Put Human Rights at the forefront of BRICS Leaders' Summit. Available at: https://amnesty.org.za/south-africa-china-put-human-rights-at-the-forefront-of-brics-leaders-summit/ (Accessed on 24 June 2024.)

Amnesty International (2023) Russia: Kremlin critic Aleksei Navalny has been sentenced to at least an additional 10 years in a penal colony. Available at: https://www.amnesty.org/en/latest/news/2023/08/russia-kremlin-critic-aleksei-navalny-sentenced-to-a-further-10-years-in-a-penal-colony/ (Accessed 12 August 2024.)

Annor, I., 09 August 2023. Can BRICS Overcome Members' Political Differences? Voice of America (VoA) Africa. Available at: https://www.voaafrica.com/a/can-brics-overcome-members-political-and-economic-differences-/7244648.html. (Accessed 14 August 2024.).

Beeson, M. & J. Zeng 2018. The BRICS and Global Governance: China's Contradictory Role. *Third World Quarterly 39*,10: 1962 - 1978. https://doi.org/10.1080/01436597.2018.1438186

Boer, R. 2022. The Concrete Conditions of Human Rights: Western and Chinese Approaches. *International Critical Thought* 12,2: 237 - 252. https://doi.org/10.1080/21598282.2022.2074512

BRICS SUMMIT 2023. Johannesburg II Declaration: BRICS and Africa: Partnership for Mutually Accelerated Growth, Sustainable Development and Inclusive Multilateralism. Sandton, South Africa. Available at: www.mea.gov.in/Images/CPV/Declaration_2408.pdf (Accessed on 21 July 2024.)

CIVICUS , 01 September 2023. BRICS: The Burgeoning of an International Repressive Alliance? https://lens.civicus.org/brics-the-burgeoning-of-an-international-repressive-alliance/

CIVICUS LENS 2023. New Members Largely a Gallery of Authoritarian States. Available at: https://lens.civicus.org/brics-the-burgeoning-of-an-international-repressive-alliance/ (Accessed 27 July 2024.)

Daniel, R. & K. Virk 2014. South Africa and the BRICS: Progress, Problems and Prospects. Centre for Conflict Resolution (CCR). https://archive.ids.ac.uk/eldis/document/A71401.html

Dixon, C. 2015. The New BRICS Bank: Challenging the International Financial Order? *Global Policy Institute Policy Paper* 28: 1 - 13.

Fairplanet. 31 August 2023. Building BRICS: Putting Human Rights on the Agenda. Available at: https://www.fairplanet.org/editors-pick/brics-human-rights-agenda/ (Accessed 27 June 2024.)

Freedom House 2023. Freedom in the World 2023: Marking 50 Years in the Struggle for Democracy. Available at: https://freedomhouse.org/report/freedom-world/2023/marking-50-years (Accessed on 03 August 2024.)

Gilbert, A. 2019. *An Analysis of the Legitimacy of the BRICS in the International System*. Pretoria: University of Pretoria, South Africa.

Glosny, M.A. 2010. China and the BRICS: A Real (but Limited) Partnership in a Unipolar World. *Polity 42*,1: 100 - 129.

Human Rights Watch 2023. World Report 2023. Available at: https://www.hrw.org/world-report/2023 (Accessed on 12 August 2024.)

Kirton, J. & M. Larionova 2022. The First Fifteen Years of the BRICS. *International Organisations Research Journal* 17,2: 7 - 30.

Li, X. & P. Steenhagen 2024. Missed Opportunity: Argentina not Joining BRICS is Likely to Prove a Costly Mistake. *China Daily* 13.

Lipton, M. 2017. Are the BRICS Reformers, Revolutionaries, or Counter-revolutionaries? *South African Journal of International Affairs 24*,1: 41 -59.

Mumuni, S.M. 2017. Chinas Non-intervention Policy in Africa: Principle versus Pragmatism. *African Journal of Political Science and International Relations* 11,9: 258 - 273.

Nuruzzaman, M. 2020. Why BRICS Is No Threat to the Post-war Liberal World Order. *International Studies* 57,1: 51 – 66. https://doi.org/10.1177/0020881719884449

Panova, V. 2021. Age of Multilateralism: Why is BRICS Important despite Possible Weaknesses? A Perspective from Russia. Global Policy. https://doi.org/10.1111/1758-5899.13013

Patnaik, A.K. 2022. Evolution of BRICS: History and Politics. In *Locating BRICS in the Global Order*. New Delhi, India: Routledge.

Pomeroy, M., A. Shankland, A. Poskitt, K.K. Bandyopadhyay & R. Tandon 2016. Civil Society, BRICS and International Development Cooperation: Perspectives from India, South Africa and Brazil. *The BRICS in International Development* 169 - 206.

Rivers, L. 2015. The BRICS and the Global Human Rights Regime: Is An Alternative Norms Regime in Our Future? Proceedings of The National Conference on Undergraduate Research (NCUR) 2015, Eastern Washington University, Cheney, WA, April 16 - 18, 2015.

https://libjournals.unca.edu/ncur/wp-content/uploads/2021/07/1453-Rivers-Lucas-Ginger.pdf

Ross, A.G. 2024. The BRICS+: Who are They, Why are They Important, and What do They Want? *Local Economy* 02690942241270551.

Staniste, M.M. 2015. Humanitarian Interventions, Responsibility to Protect versus State Sovereignty: The BRICS Countries Perspectives. *International Journal on Humanistic Ideology* 6: 57.

Singh, B.P. 2019. Does Governance Matter? Evidence from BRICS. Global Business Review 23,2: 408 - 425. https://doi.org/10.1177/0972150919861222

Subedi, S. 2015. The Universality of Human Rights and the UN Human Rights Agenda: The Impact of the Shift of Power to the East and the Resurgence of the BRICS. *Indian Journal of International Law* 55: 177 - 207.

Ullah, I., S.M. Haider & M. Gohar 2024. BRICS Expansion: Prospects and Challenges. *Research Journal of Human and Social Aspects* 2,1: 52 - 64.

United Nations, Office of the High Commissioner for Human Rights 2022. Country Reports: OHCHR Assessment of Human Rights Concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China. Available at: https://www.ohchr.org/en/documents/country-reports/ohchr-assessment-human-rights-concerns-xinjiang-uyghur-autonomous-region (Accessed 25 June 2024.)

Varela, A. & R.G.M. Delgado 2019. The BRICS in the Contemporary Global Order: Objectives, Capabilities, and Limitations. *Otoritas: Jurnal Ilmu Pemerintaha* 9,2,October: 89 – 106.

Simbarashe Tembo
University of Fort Hare
Stembo@ufh.ac.za

James Ndlovu
Durban University of Technology
Jamesn@dut.ac.za

# Chapter 10: An Exploratory Study on the Transnational Illicit Drug Trade and its Dangers to BRICS Countries – A Scoping Review

**Sandhya Maharaj**
**ORCID iD: https://orcid.org/0009-0006-2670-2547**

## Abstract

Drug addiction is a global scourge and is a threat to human survival. The United Nations in its World Drug Report (UNODC 2024a) states that almost 292 million people used drugs in 2022 – a 20% increase from 2012. This study examines the prevalence and impact of transnational illicit drug trafficking in BRICS countries. Brazil, Russia, India, China and South Africa are the original members of BRICS-a formidable political and economic alliance. A study examining the growth and prevalence of illicit drugs in these regions is therefore necessary. Rapid modernisation, urbanisation and migration has reshaped drug trafficking patterns and addiction. This scoping review seeks to investigate the trade effects on public health, economic stability and social cohesion within BRICS jurisdictions.

It is imperative that the inflow of illicit drugs is stopped. This necessitates the formation of a cohesive partnership of BRICS nations. A strong and strategic alliance with a co-ordinated anti-drug strategy is the only viable solution to combat transnational drug trafficking.

The scoping review further indicates that transnational illicit drug trafficking in BRICS countries is widespread and presents serious challenges across public health, security, and governance. The prevalence of drugs like cocaine, heroin, methamphetamines, and synthetic opioids significantly impacts these countries, with the consequences spilling over into regional and global security. Despite the implementation of anti-drug trafficking policy responses, difficulties associated with corruption, resource constraints, and complex international trafficking networks constitute a major hurdle in the fight against drug trafficking. The dangers to public health caused by illicit drug use, such as

the spread of HIV, should sound the alarm bells amongst BRICS. A unified BRICS response, spanning the four strategically located regions is vital in combatting the rising drug threat.

**Keywords:** illicit drugs; drug trafficking; transnational; users who inject; HIV; BRICS, heroin, cocaine, fentanyl, precursor chemicals

## Introduction

The BRICS countries—Brazil, Russia, India, China, and South Africa—represents a variety of emerging economies with substantial geopolitical influence. In 2022, the combined GDP of BRICS nations amassed to 25.85 trillion US dollars representing 35% of the global GDP while G7 countries account for 30% (*The Globalist* 2024). The countries forming part of the BRICS nations are key players politically and economically. Each of the countries exert a strong influence in their respective regions.

However, these nations must be wary of an emerging threat from transnational illicit drug trafficking. This desktop review discusses the prevalence of transnational illicit drug trafficking in BRICS countries, its impact, and policy responses. This scoping review highlights the serious challenges the illicit trade poses to BRICS nations, emphasizing the need for international cooperation and a focus on harm-reduction strategies.

The global drug trade has evolved to become pervasive and complex and must be considered a clear and present danger to all BRICS nations. Internal security and economic well-being will undoubtedly be affected by sprouting organized crime in the form of the drug trade.

## Drug Addiction: A Global Scourge

Drug addiction is a threat to human survival (Saah 2005), the United Nations in its World Drug Report states that almost 292 million people used drugs in 2022; this is a 20% increase from 2012. Difficulties in eradicating drug use centre around the sheer variety of drugs available with differing modes of intake. Globally the number of drug users is expected to rise by 40% by the year 2030 (UNODC 2023). Rapid modernisation, urbanisation and migration, have changed patterns of drug trafficking and addiction.

In May 2024, the BRICS anti-drug working group held a summit in Moscow where heads of State representing the various BRICS nations discussed the global rise in drug trafficking. The need for increased international cooperation was emphasised (Russian Ministry of Internal Affairs 2024).

This scoping review will explore:

- The prevalence of transnational drug trafficking in BRICS countries.
- The types of drugs trafficked across borders within and outside these nations.
- Impact of Drug Trafficking on Public Health and Social Security.
- Policy responses.

## Prevalence of Transnational Drug Trafficking in BRICS Countries

BRICS nations are deeply intertwined in the global illicit drug trade due to their strategic geographical positions and economic participation. Geographical factors greatly influence the vulnerability of BRICS nations to drug trafficking, especially in coastal areas. Countries like South Africa, India, and China with extensive coastlines are prime targets for drug cartels, as these regions facilitate maritime smuggling.

**Brazil**, positioned close to the leading cocaine-producing nations of Colombia, Peru, and Bolivia, plays a crucial role in the global cocaine trade, making it the second-largest producer after Colombia. Brazil's porous borders with Argentina and Paraguay further complicate law enforcement efforts to curb drug trafficking. Brazil's location near the Amazon and Colombia's drug-producing regions positions it as a major transit hub and an essential transit point for narcotics destined for markets in Europe, Africa, and Asia. Maritime routes are significant in this commerce, with around 90% of cocaine departing South America through Brazilian ports (Proinde 2023). Despite rigorous law enforcement efforts and heightened oversight, drug trafficking activities in Brazil are on the rise, fuelled by the nation's vast coastline and the growing number of ports that aid the operations of organized crime groups (Geldenhuys 2024).

**Russia,** a similar increase can be observed in Russia where the heroin trade is largely influenced by trafficking networks originating from Afghanistan,

passing through Central Asia. In 2020, authorities in Russia intercepted 2.4 tons of heroin (UNODC 2024b). Russia has one of the highest rates of heroin consumption worldwide, with an estimated 2.5 million users (Hellman 2022).

Alarmingly, there has been a marked pivot towards synthetic drug use in Russia, especially cathinones, which are manufactured domestically and are often more easily accessible and economically viable compared to traditional narcotics. Russia has witnessed a new method of drug trafficking, the rise of the 'dead drop' distribution method. The 'dead drop' system is facilitated by the dark web and utilising the anonymity of cryptocurrency payments benefiting both the distributor and the consumer. This innovation has significantly contributed to the proliferation of drug trafficking through digital platforms, complicating enforcement efforts (Daly & Shortis 2024)

**India**, plays a significant role as both a producer and transit corridor in the drug trade, especially for heroin from Afghanistan and methamphetamines from Southeast Asia. In 2020, Indian authorities confiscated over 3.5 tons of heroin (UNODC 2024b). This highlights proactive efforts against an escalating opioid crisis that affects around 2.1% of the population due to proximity to the Golden Crescent (Athawale 2021).

**China,** is a major source for synthetic drugs like methamphetamines and fentanyl seizing approximately 18 tons of methamphetamine in 2020 (UNODC 20 24) emphasizing the need for international collaboration in drug control. The U.S. has identified both India and China as key hubs in the transnational drug trade for fiscal years 2024 and 2025 (White House Memorandum 2025).

**South Africa** acts as a key trafficking hub for cocaine, methamphetamines, and heroin, with over 2.5 tons of cocaine seized in 2020 (UNODC 2024b). The 2023 - 2024 South Africa Police Service statistics highlight severe impacts from drug influxes, with 3,747 arrests for drug dealing and millions of rands seized in cocaine (SAPS Crime Statistics 2023/2024). It is estimated 15% of the population suffers from addiction, surpassing the global average. While strategically positioned for narcotics trafficking between South America, Asia, and European markets, South Africa faces challenges due to its porous borders and maritime smuggling necessitates improved law enforcement strategies (Eligh 2021).

Furthermore, rising methamphetamine use, especially among the youth is contributing to violence and health risks. The trafficking of diverse illicit drugs is increasing, targeting various socio-economic backgrounds and making

eradication efforts challenging (Eligh 2021). Post-apartheid South Africa has attracted drug cartels, using the region as a link to global markets (Shereda 1997 - 1998).

## Classes of Drugs Trafficked across Borders Within and Outside BRICS Nations

The demand for illicit drugs trafficked in BRICS countries reflects the dynamics of local and international markets. One of the key findings of the United Nations World Drug Report (2024a) indicates that the types of illicit drugs available on the global market have diversified and this has complicated anti-drug initiatives. Commonly trafficked drugs across these nations include:

**Heroine** produced in the 'Golden Triangle' and 'Golden Crescent', which traverses the borders of Pakistan, Afghanistan, and Iran, account for a significant percentage of the world's heroin supply (Gerry & Sherwill 2016). Most of the opium cultivated in the Golden Crescent is smuggled into the United States (Barnett 1985). Over 80% of the world's heroin is supplied by Afghanistan and smuggled throughout the world using routes through BRICS jurisdictions (Chin & Zhang 2015).

**Cocaine** cultivated in South America and smuggled through Brazil and South Africa to Europe. Brazil is experiencing a rampant public health crisis in the form of crack cocaine use. In 2020, Brazil seized over 25 tons of cocaine. Addiction to crack-cocaine drug is the cause of various forms of psychiatric and psychosocial issues. A disruptive or chaotic family environment is one of the risk factors contributing to the rise of crack cocaine (Perrenoud *et al.* 2021). High rates of HIV, hepatitis B and C are prevalent among users of crack cocaine. Furthermore, studies indicate that homicide is the leading cause of death among users of crack cocaine in Brazil (Perrenoud *et al.* 2021).

**Cannabis** is still the most common drug used in Africa. However, this is slowly changing as the demand for heroin, cocaine, and synthetic drugs such as methamphetamine grows. The drug Methaqualone (Mandrax) was the most common synthetic drug until it was dethroned by methamphetamine. This can be attributed to the drug infiltrating the local market while transiting through Africa on its way to Europe (UNODC 2024c).

**Synthetic Opioids: Fentanyl**, in recent years, synthetic opioids like fentanyl—known as the synthetic cousin of heroin—have emerged as a major threat, with trafficking channels mainly flowing from China to the United States and Europe. The United States reports that their Customs and Border Protection has prevented the entry of more Fentanyl in the last two years than in the last five years combined (White House Memorandum 2025)

In 2023, US Customs and Border Protection seized 1.2 billion doses of Fentanyl. Fentanyl use and trafficking have the potential to cause a global crisis if not controlled. The United States has entered a global coalition consisting of 150 countries to address synthetic drug use. Illicit drug use and trafficking have increased globally; a trilateral Fentanyl Committee consisting of Canada, Mexico, and the United States has been formed to prevent the flow of pre-cursor chemicals used to manufacture synthetic drugs like Fentanyl, which is 80 times more powerful than morphine and 50 times stronger than heroin (White House Memorandum 2025). A dose of 3 mg of Fentanyl is enough to kill an adult human. Traffickers are mixing Fentanyl with heroin, making the two drugs hard to differentiate. The mixing of dangerous drugs is contributing to high mortality rates among users.

The rise of and popularity of synthetic drugs, which are more widely available, is a serious threat. Controlling the illegal entry of illicit drugs into a jurisdiction is not enough; traffickers smuggle in chemicals necessary for heroin, cocaine and various synthetic drug production. Countries worldwide, led by the United States, have committed to stop the trafficking of precursor chemicals (US Department of State Dispatch: Fact Sheet No 9 1992).

## Impact on Public Health and Social Security: The Rise of HIV in Users Who Inject Drugs

There is a notable rise in HIV transmission among individuals who inject drugs. Unsafe drug use methods significantly increase the risk of HIV spread, with around 13 million people injecting illicit drugs globally, mostly from developing nations, and an estimated 10% living with HIV (UNAIDS 2021).

## In BRICS

**Brazil**, the proportion of HIV/AIDS cases among injecting drug users dropped from 17% in 1980-1997 to 2.1% due to harm reduction initiatives like needle exchange programs (Guimarães 2015).

Conversely, **Russia** struggles with high heroin addiction rates, with about 2% of the population affected. This contributes to severe health issues, including a rise in HIV and hepatitis C cases. In 2022, drug overdoses surged by 16% from 2019, with 18,013 reported cases (Hellman 2022). The link between intravenous drug use and HIV transmission needs more attention as the number of HIV positive individuals in Russia is estimated to be close one million (Lunz *et al.* 2017 and Edelman *et al.* 2017).

In **India**, the opioid epidemic is contributing to high rates of heroin addiction and overdose deaths. Injecting drug use is a major factor in HIV transmission, with an estimated 6.23% of approximately 20,000 users infected (Pachuau *et al*. 2022). Initial prevention efforts focused on sex workers after HIV was first detected in 1986, neglecting the risks posed by unsafe needle practices among drug users. Although HIV rates among sex workers have decreased, rates of HIV have risen among injecting drug users, particularly in Northern India near the 'golden triangle' (Pachuau *et al.* 2022).

In **China,** over half of HIV-positive individuals are injectable drug users, with high transmission rates linked to needle sharing near opium-rich areas (Levitsky 1992). The popularity of intravenous drug use has surged along southern borders adjacent to countries like Burma and Thailand. China reported its first HIV case in 1985, with cases growing to 850,000 by 2016 (Meng 2016). The government has since implemented various prevention and treatment strategies including harm reduction strategies.

**South Africa -** despite the implementation of the largest anti-retroviral therapy programs, only 40% of HIV-positive injecting drug users access treatment. Stigmas around HIV and the high rates of alcohol and cannabis use further complicate health outcomes, drug use is linked to higher rates of unprotected sex and increased HIV transmission risks (Browne *et al.* 2010).

The HIV epidemic remains a significant crisis, with South Africa being at the epicentre of the epidemic. The correlation between substance abuse and the spread of HIV and HCV is troubling, particularly as drug users are found to be at a higher risk of engaging in unprotected sex, thus amplifying the ongoing health challenges. Users of injectable drugs are also engaging in dangerous practices such as 'blue toothing' (Zanoni *et al.* 2023).

In the UNODC 2005 report, the sharing of needles by drug users was common (Parry *et al.* 2008). Statistics show that the popularity of injectable

drugs such as cocaine and heroin has grown steadily. There is a real danger that different modes of substance abuse, namely injecting drugs and sharing needles, can cause an upsurge in HIV transmission.

The United Nations, in its UNAIDS Report 2021, stated that HIV prevention amongst drug users is an area of priority. Browne *et al.* states that HIV prevention programmes must seriously address the growing intersection of the risk of substance use, violence and HIV risk in South Africa (Browne *et al.* 2010). Investigating the link between drug intake and HIV is important as it determines how programmes designed to cut transmission of HIV should operate.

## Economic and Social Impact

Drug addiction has a profound impact on society, affecting individuals in their prime who could otherwise contribute positively to the economy and society at large. This dependency transforms potential contributors into liabilities, placing burdens on families and straining state resources. Countries that serve as transit hubs for illicit drugs are especially vulnerable to corruption, worsening social and economic challenges for citizens. Additionally, poverty is a key factor driving the growth of the illicit drug market, leading to public health crises, particularly in Eastern and Southern Africa, due to ineffective strategies against drug proliferation in the region.

While countries grapple with the impending drug threat, the transnational illicit crime network has grown bigger and stronger, fending off various anti-drug initiatives. Proof of this problem lies in the statistics, which indicate that as many as 250,000 drug-related deaths occur annually throughout the world. Drugs originating in Asia and South America are trafficked all over the world (UNODC 20 24a)

Trafficking networks spawn from the growth of corruption in governmental structures. Corruption spurred by drug trafficking undermines the rule of law and equality in the distribution of wealth within the society and compromises the legitimacy of governmental arms (Ekici 2014 discussing Williams 2007).

### *Social Instability*

The transnational drug trade aids organized crime, violence, and instability, particularly in regions with weakened government structures. The illicit drug

trade undermines governance especially in transit hubs like Eastern and Southern Africa. This leads to the erosion of societies through disharmony and chaos in the form of increased violent and non-violent crime. Substance abuse is a contributing factor in 40%-60% of domestic violence incidents (Martens 2024).

## *Security Risks*

The transnational nature of the drug trade poses significant security challenges. The increase in population size globally, as well as socio-economic factors, are contributors. The trafficking of drugs is an intricate web of organised crime which lacks a definite structure. Drug trafficking can vary in many ways, from the type of product they peddle to how they interact and integrate into society (Eligh 2021)

Due to the versatility of drug trafficking patterns, combatting the drug scourge has been difficult. Drug trafficking is a covert silent killer which ultimately causes the degradation of society. The veiled operations may undermine political instability and territorial vitality and harm economic development. Drug networks are opportunistic and take advantage of weak borders. Despite stringent border controls, traffickers cleverly circumvent these obstacles (Ekici 2014).

## *Policy Responses*

Governments in BRICS countries have adopted varying approaches to combat the illicit drug trade, with varying degrees of success. To prevent drug addiction within a society, many countries have implemented stringent border controls. Geographically vulnerable countries in Eastern and Southern Africa are examples of regions which play a prominent role in the illicit transit of narcotics (Barnett 1985). Infrastructure development in these areas also contributes to the increase in market demand. One of the adverse effects of globalisation is the growing popularity of illicit drugs due to migration, urbanisation and the advancement of technology.

Gardner argues that domestic solutions alone to the international drug trade are inadequate against complex, well-run, organised syndicates that violate international law and international boundaries (Gardner 1993).

**Brazil**'s anti-drug operations are heavily focused on seizing drugs at borders

and intercepting traffickers in ports and airports. However, corruption and lack of infrastructure complicate efforts (Geldenhuys 20 24).

**Russia** has transformed due to its geopolitical context and relations with Western nations, especially after the war with Ukraine in 2022, this has led to significant sanctions from the European Union and other countries. The political turmoil in the region has resulted in the development of a new model for drug trafficking (Daly & Shortis 2024).

This new model is considerably more efficient and poses greater risks. The dead drop system has surged in Russia due to the country's highly tech-savvy population and offers delivery over long distances. This method of trafficking has led to an increase in the distribution of synthetic drugs compared to previous years. It not only facilitates the distribution of illegal substances but also encourages dealers to create synthetic drugs (Daly & Shortis 2024)

According to Daly and Shortis (2024), cartels can no longer depend on imports because of sanctions, forcing them to produce their own drugs. To achieve this, these cartels rely on precursor chemicals imported from India and China. This emerging method of drug trafficking poses a significant threat not only to Russia but also to the global community. Evidence suggests that this approach is already spreading to Asia and Europe, making it an urgent issue.

**India** has initiated measures such as the National Drug Control Policy to combat the trafficking of opioids. Cooperation with neighbouring countries, such as Afghanistan and Myanmar, is key. In 1999, the Indian government made a concerted effort to strengthen border controls; however, India still faces a growing drug epidemic. In 1979, pricier drugs such as heroin lacked in popularity because of widespread poverty. The advent of a stronger economy now sees the popularity of more dangerous drugs such as cocaine and heroin. The use of these drugs has contributed to the increase in the spread of HIV (Mitra 2004).

**China** has ramped up its efforts against synthetic drug production, particularly fentanyl, but enforcement is challenging due to the scale of production and the international nature of trafficking. Nonetheless, China takes a tough stance on drugs, often executing drug mules who are found with large amounts of illegal narcotics. Traffickers and those convicted for manufacturing organised crime also attract the death penalty. Additionally, individuals who are identified as

drug users are sent to mandatory detoxification centres. Thus, China has been criticised for its stringent stance on drug users, with critics arguing that these methods constitute an abuse of human rights while still being ineffective at treating drug use. A successful approach should combine social support and provide for psychosocial treatments (Yang & Giummarra 2021).

China, Iran, Saudi Arabia, Vietnam, Malaysia and Singapore are countries that punish drug trafficking with the death penalty (Gerry & Sherwill 2016). China has taken a zero-tolerance policy on drugs and, as a result, enjoyed 30 drug-free years from 1950 till the 1980s. However, there was a downward turn from the 1990s till 2005, when 1 million drug users were registered (Gerry & Sherwill 2016). One of the features of the illicit drug trade is 'group offending'; this means that trafficking involves a host of different operators, from wholesalers to retailers and runners (Spencer *et al.* 2015) Therefore, tackling the illicit drug trade is particularly difficult. From this period, illicit drug use steadily increased despite strict anti-drug laws. If an individual is found with more than 50g of illicit drugs, they risk being sentenced to death. Notably, drug-related executions have increased in certain regions, including Iran, Indonesia and China (Gerry & Sherwill 2016)

China has made great strides in curbing the spread of HIV by addressing the spread of the virus in high-risk groups such as drug users who inject. A two-prong approach, the first involves the strict policing of drugs and the second focuses on harm reduction in the drug users. The clean needle programme and methadone maintenance form part of the harm reduction initiative. Harm reduction initiatives are necessary and complementary to policing. In China, this strategy has seen success. Meng argues that the sex industry must be decriminalised to ensure that China's HIV prevention and treatment programmes are more effective (Meng 2016)

**South Africa**'s Drugs and Drug Trafficking Act 144 of 1992, promulgated in April 1993, was enacted to tackle the booming international trade in drugs. The Act introduced into the South African law measures adopted by the international community designed to suppress the international drug trafficking market (Boister 1995) The United Nations Convention against Illicit Drug Traffic in Narcotics Drugs and Psychotropic Substances influences the Act (UN Document E/CONF.82/15 of 19 December 1988 cited by Milton 1993). In 2020, the South African government launched the National Drug Master Plan (2020) to tackle substance abuse, which has reached alarming proportions.

The emergence of organised crime in the form of drug trafficking was

a relatively new problem in post-apartheid South Africa. Shielded and isolated from the global stage, the reign of democracy exposed the region to the world of organised crime (Shereda 1998). South Africa has since become the regional hub for various types of organised crime, particularly illicit drug trafficking. South Africa serves as a major transit hub and has become a major drug market (Eligh 2021)

South Africa has a comprehensive drug control framework, however drug-linked violence and inadequate resources hamper its success. Eligh asserts that corruption of domestic law enforcement institutions may be the strongest structural enabler of the illicit drug trade in the Eastern and southern regions of Africa. In cases where there is no corruption, law enforcement agencies simply lack the capability and capacity to tackle this issue. These factors, coupled with the geographical location of Eastern and Southern Africa, make the flow of the illicit trafficking of drugs easier (Eligh 2021).

Despite the increase in the seizure of drug consignments in various regions, drug cartels are able to stay steps ahead of anti-trafficking initiatives (Eligh 2021). Drugs are also being sold at lower prices, making them more attainable to larger parts of the population, thereby essentially 'infecting' society with drug addiction. Eligh states that the current approach to combatting illicit drug trafficking in the Eastern and Southern regions of Africa has been inadequate. Reformation of policy and legislation by itself is falling short of combatting the drug problem because it is not multi-dimensional and cannot dismantle complex drug syndicate structures.

## Research Methodology

The methodology for reviewing the literature on transnational drug trafficking in BRICS countries involved scoping review utilising desktop research. A systematic review of existing secondary data from available literature and online databases was conducted. This was useful for mapping complex topics and identifying key themes and research gaps guided by Arksey and O'Malley's (2005) five-stage framework, with Levac *et al.* (2010) enhancing the study's rigour to map transnational drug trafficking in BRICS countries.

**The stages included:**

1. Defining the research question.
2. Identifying relevant studies.
3. Selecting studies.
4. Charting the data.
5. Collating and reporting the results.

## *Stage 1: Defining the Research Question*

The Population, Concept, and Context (PCC) Framework from the Joanna Briggs Institute (2021) was utilized to define the review's research question and focus, as illustrated in Table 1.

**Table 1: PCC Framework**

| Population | Concept | Context |
|---|---|---|
| BRICS Countries | Transnational drug-trafficking | Global |
| Brazil | Drug-smuggling | International |
| Russia | Drug-trade | Worldwide |
| India | Illegal drugs across borders | |
| China | Illegal drug transportation | |
| South Africa | Heroin/Opiates | |

## *Stage 2: Identifying Relevant Studies*

According to Arksey and O'Malley (2005), a systematic search strategy is essential for gathering relevant literature that addresses research questions. For this study, literature was sourced from academic databases, reference lists, key journals, and government organizations related to drug policy and enforcement. Databases used included Google Scholar, JSTOR, and ScienceDirect. Additionally, reports from the UNODC, INTERPOL, and World Customs Organization were reviewed to investigate transnational drug trafficking in BRICS countries. Sources were evaluated for credibility, relevance and recency. Priority was given to peer-reviewed publication and authorities reports.

The search included various study designs—qualitative, quantitative, mixed-methods, and grey literature – focusing on studies published in English since 2010, coinciding with the BRICS countries' formalization and the resulting academic interest in their impact on political and cultural dynamics (DIRCO 2014).

## Search Terms and Strategy

To guide this study, search terms were developed to capture the diverse aspects of the topic. The keywords included:

BRICS countries OR Brazil OR Russia OR India OR China OR South Africa AND Transnational drug-trafficking OR Drug-smuggling OR Trade OR Illegal drugs across borders OR Illegal drug transportation OR Heroin OR Opiates Or Heroin and HIV and Injecting drug use AND Global OR International OR Worldwide.

A pilot search was conducted on Google Scholar to ensure the feasibility of the selected keywords (refer to Table 2 below).

**Table 2. Pilot Search Database Results**
**Of the 2540 hits obtained, 240 were included after screening.**

| Date of Search | Keyword Search | Publications Retrieved | Search Engine Utilised |
|---|---|---|---|
| 11 December 2024 | (BRICS countries OR Brazil OR Russia OR India OR China OR South Africa) AND (Transnational drug-trafficking OR Drug-smuggling OR Drug-trade OR Illegal drugs across borders OR Illegal drug transportation OR Heroin OR Opiates and HIV and Injecting drug use AND (Global OR International OR Worldwide) | 2 540 | Google Scholar |

## *Stage 3: Study Selection*

To ensure a comprehensive scoping review aligned with research objectives, Arksey and O'Malley (2005) emphasize the importance of selecting articles using explicit inclusion and exclusion criteria. This approach minimizes bias and ensures findings are based on systematically reviewed evidence. Table 3 outlines the criteria applied during the title, abstract, and full-text screening stages to identify studies relevant to the research questions.

After the identification of the relevant criterion, the evaluation of the titles and abstracts of the studies identified in the previous stage was conducted.

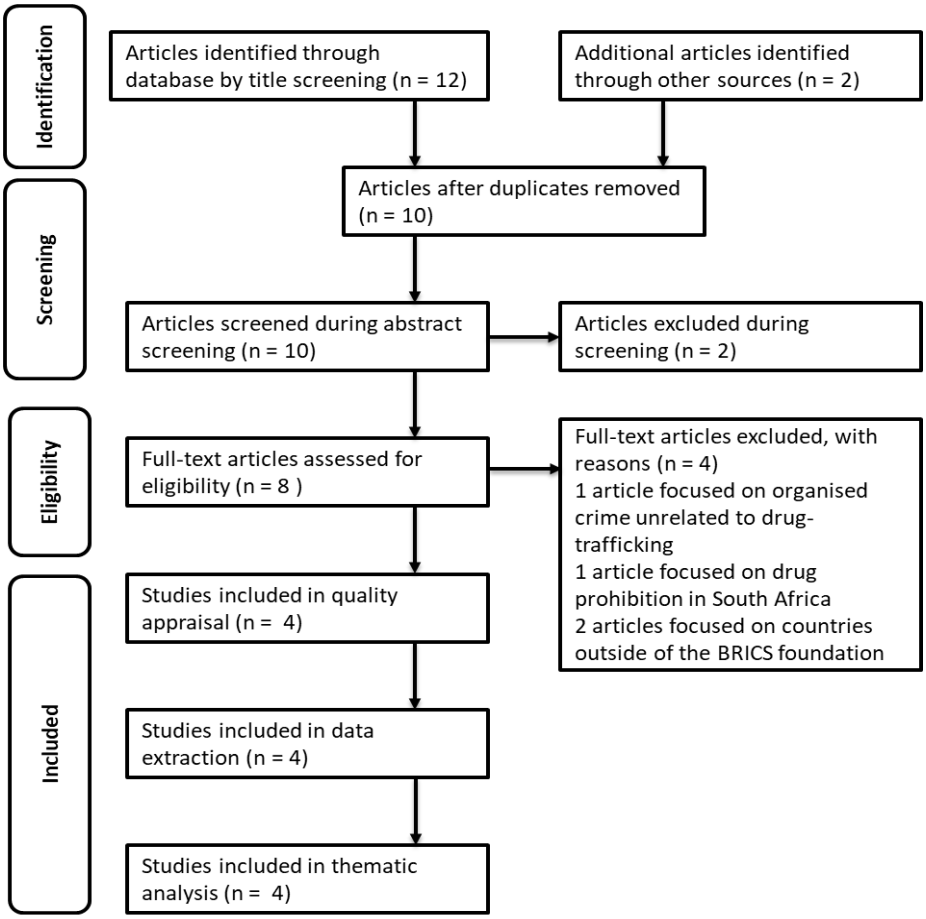
This was followed by a more thorough evaluation involving a review of the full texts of the selected studies to assess their relevance to the criteria, with reasons for exclusion documented as needed. Ultimately, PRISMA guidelines were used to document the selection process to maintain transparency. Figure.1 below presents a PRISMA flowchart illustration the study selection process. With a clearly defined set of relevant studies, the data collected was more consistent, facilitating the identification of themes and patterns aligned with the research objectives and questions.

**Table 3. Inclusion and Exclusion Criteria**

| Criteria | Inclusion Criteria | Exclusion Criteria |
|---|---|---|
| Population | Studies focusing on BRICS countries | Studies unrelated to BRICS countries |
| Concept | Studies addressing transnational drug-trafficking | Studies unrelated to drug-trafficking |
| Context | Studies within a global framework but focused on BRICS countries | Studies outside the scope of BRICS countries or unrelated global contexts |
| Study design | Qualitative, quantitative, mixed-method studies, and grey literature. | Opinion pieces without empirical data or analysis |
| Language | English publications | Non-English publications |
| Period | Articles published from 2010 onwards | Articles published before 2010 |

Studies focusing on non-BRICS nations were excluded. Themes not related to drug trafficking were excluded. Opinion pieces lacking empirical data was excluded.

**Figure 1. PRISMA Flowchart Diagram**




## *Stage 4: Charting the Data*

Data extraction follows study selection and is performed using a standardized form to ensure consistency and accuracy (Arksey & O'Malley 2005). This systematic approach is essential for identifying relevant studies and analysing findings, providing a solid foundation for summarizing results. An example of the data extraction form is shown in Table 4.

**Table 4. Data Charting Tool**

| |
|---|
| Citation details |
| Study design |
| Geographic region |
| Study population |
| Aim/Research question |
| Key findings |

### *Stage 5: Collating, Summarising, and Reporting the Results*

Braune and Clarke (2006) championed thematic analysis for synthesizing qualitative data during the study selection process, especially given the large volume of information involved. This method allows researchers to identify recurring themes relevant to their research questions and comprises six phases: familiarization with data, coding, theme organization, theme review, significance establishment, and reporting findings. In this study, thematic analysis effectively examined the complexities of transnational drug trafficking in BRICS countries. The themes were not predetermined to maintain objectivity, with the researcher's focus aligned with the aims and questions regarding drug trafficking dynamics and implications in these nations.

## Quality Appraisal

Quality appraisal, as recommended by Levac *et al*. (2010), involves systematically assessing the validity of articles in a review. For this study on transnational drug trafficking in BRICS countries, the Mixed Method Appraisal Tool (MMAT) was utilized due to its comprehensive framework for evaluating both qualitative and quantitative studies. Appraisal criteria focused on the clarity of research design, alignment of research questions with objectives, and rigor of data collection and analysis. This approach enhanced the overall reliability and validity of the scoping review.

## Findings

This review reveals the that transnational illicit drug trafficking a complex problem and demands urgent attention. BRICS nations have adopted diverse approaches to combat drug trafficking, each facing unique challenges and achieving varying levels of success. The solution to this problem must encompass a co-ordinated strategy by BRICS nations. A multi-pronged strategy wherein BRICS countries partner and collaborate with each other with the sole focus of eradicating transnational drug trafficking from its point of origin to its various destinations.

**Brazil** has primarily concentrated on seizing drugs at borders and inter-cepting traffickers, targeting ports and airports. However, seizing contraband at the ports and borders is not, on its own an effective long terms solution.

**Russia** is grappling with a substantial heroin influx, and has therefore stepped-up enforcement against trafficking, however the sheer volume of drugs entering the country, compounded by organised crime, poses persistent obstacles. This review further stresses the importance of a strategy developed to address the use of technology to facilitate drug trafficking. Cyber security and technology must be enhanced to stay abreast with the rapid evolution of drug trafficking both domestically and globally. It is clear, countries such as Russia have fallen prey to the technology driven 'dead drop' system which spells a new age of drug trafficking and has the potential to spread to various jurisdictions. This system, facilitated by the dark web and cryptocurrency, underscores the need for governments to embrace technological advancements in their counter-narcotics efforts.

**India** has taken a multifaceted approach, enacting the National Drug Control Policy and prioritizing collaboration with neighbouring nations like Afghanistan and Myanmar to curb the opioid trade. Despite these measures, India still grapples with a burgeoning drug epidemic, which has evolved from the use of less expensive drugs in the past to more potent, dangerous and expensive substances like cocaine and heroin, contributing to the spread of HIV. This strongly indicates that a stronger economy may not necessarily spell the end of substance abuse but facilitate use of more expensive drugs in countries such as India.

**China** stands out with its stringent zero-tolerance policy on drugs, enforcing harsh penalties, including the death penalty for drug trafficking and mandatory detoxification for users. While credited with controlling drug use for three decades (1950s - 1980s), this approach has been criticized for its potential human rights violations and limited efficacy in addressing addiction. China's harm reduction initiatives, such as needle exchange programs and methadone maintenance, have proven successful in curbing HIV transmission among injecting drug users.

Urgent attention must be given to the public health crisis created through injecting drug use. BRICS countries must attend to this grave threat. Harm reduction initiative must be implemented where injecting drug use is prevalent. If injecting drug use is not contained, many BRICS nations may experience a new wave in the spread of HIV. Countries such as India and South Africa must be wary of the dangers inherent with increasing injectable drug use amongst the HIV positive population.

**South Africa**, operating under the Drugs and Drug Trafficking Act of 1992 and the National Drug Master Plan, faces challenges from drug-related violence and resource constraints. The nation's emergence as a regional hub for drug trafficking is attributed to its strategic location and the exploitation of vulnerabilities in its post-apartheid transition. Harm reduction initiatives such as needle exchange programme must be adopted in all regions where there is injectable drug use such as India and South Africa.

## Conclusion

The trafficking of drugs into certain regions can have catastrophic effects on society if not contained. A major concern is the link between HIV transmission and injecting drug users, who exhibit higher HIV rates compared to non-users. This issue demands urgent attention as neglecting it could lead to high transmission rates, even in countries that have successfully controlled the spread of HIV1. For instance, countries like India and China, with populations exceeding a billion, face significant risks if HIV transmission rates increase even slightly.

Research has identified injecting illicit drugs as a driving factor in the global HIV epidemic. The introduction of injectable drugs like heroin into regions like South Africa and India, where they were previously uncommon, highlights the emergence of new target markets.

Efforts to curb the influx of illicit drugs must also focus on preventing the entry of precursor chemicals, which enable drug manufacturing anywhere, circumventing border controls. The escalating abuse of synthetic opiates like Fentanyl requires close monitoring. Collaboration among BRICS nations is crucial to protect their respective regions. A unified front among these countries, strategically positioned across four major continents, can effectively disrupt the operations of the transnational drug trade.

## References

Arksey, H. & L. O'Malley 2005. Scoping Studies: Towards a Methodological Framework. *International Journal of Social Research Methodology* 8,1: 19 - 32. https://doi.org/10.1080/1364557032000119616

Athawale, A.P. 2021. *Legal Provisions for Proclivities of Illegal Drug Trafficking in India: NDPS Act. International Journal of Law Management & Humanities* 4, 2: 413 - 418. Available at: https://ijlmh.com/publications/volume-iv-issue-ii/ (Accessed on 22 November 2024.)

Barnett, R.J. 1985. Extradition Treaty Improvements to Combat Drug Trafficking. *Georgia Journal of International and Comparative Law* 15, 2: 285 - 316. Available at: Extradition Treaty Improvements to Combat Drug Trafficking. by J. Richard Barnett (Accessed on 22 November 2024.)

Behsat, E. 2014. International Drug Trafficking and National Security of Turkey. *Journal of Politics and Law* 7, 2: 113 - 126. (PDF) International Drug Trafficking and National Security of Turkey (Accessed on 23 November 2024.) https://doi.org/10.5539/jpl.v7n2p113

Braun, V. & V. Clarke 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 3,2: 77 - 101. https://doi.org/10.1191/1478088706qp063oa

Browne, F.A & W.M. Wechsberg 2010. Intersecting Risks of Substance Use and HIV Risk among Substance-using South African Males and Females. *Current Opinion in Psychiatry*. Available at: The intersecting risks of substance use and HIV risk among substance-using South African males and females - PMC (Accessed on 25 November 2024.) https://doi.org/10.1097/YCO.0b013e32833864eb PMid:20308902 PMCid:PMC3784346

Chin, K.L. & S.X. Zhang 2015. The Chinese Heroin Trade: Cross-border Drug

Trafficking in Southeast Asia and Beyond. In Chin, K-L. & S.X. Zhang (eds.): *The Chinese Heroin Trade.* DeGruyter & Oxford University Press. https://doi.org/10.18574/nyu/9781479865574.001.0001

Clarke, C.P. 2016. *The Global Illicit Trade in Illegal Narcotics.* In OECD. *Illicit Trade: Converging Criminal Networks.* Paris: OECD Publishing. https://doi.org/10.1787/9789264251847-9-en

Daly, M. & P. Shortis 2024. *Breaking Klad Russia's Dead Drop Drug Revolution. Global Initiative against Transnational Organised Crime*. Breaking Klad: Russia's Dead Drop Drug Revolution | Global Initiative (Accessed on 19 November 2024.)

Department of International Relations and Cooperation (DIRCO) 2014. *BRICS: Fifth Anniversary Academic Forum Booklet.* Available at: https://www.dirco.gov.za/wp-content/uploads/2023/02/bricks__fifth_book2014.pdf (Accessed on 11 December 2024.)

JBI 2021. JBI Manual for Evidence Synthesis.

Eligh, J. 2021. *Illicit Drug Markets of Eastern and Southern Africa – An Overview of Production, Supply and Use*. Eastern and Southern Africa Commission on Drugs. (PDF) Illicit drug markets of Eastern and Southern Africa: An overview of production, supply and use | Jason Eligh - Academia.edu (Accessed on 19 November 2024.)

Gardner, A.S. 1993. A Global Initiative to Deter Drug Trafficking: Will Internationalizing the Drug War Work? *Temple International and Comparative Law Journal* 7, 2: 287-318. International cooperation on drug trafficking: 10 more years of the same? | Global Initiative (Accessed on 23 November 2024.)

Geldenhuys, K. 2024. DRUGS … Know NO Borders. *Servamus Community-based Safety and Security Magazine* 117,3: 10 - 15. https://journals.co.za/doi/abs/10.10520/ejc-servamus_v117_n3_a4

Gerry, F. & N. Sherwill 1992. Human Trafficking, Drug Trafficking, and the Death Penalty. *Indonesia Law Review* 6, 3: 265 - 282. Human Trafficking, Drug Trafficking, and the Death Penalty - Charles Darwin University (Accessed on 23 November 2024.)

Gill, B., J. Chang & S. Palmer 2002. China's HIV Crisis. *Foreign Affairs* 81,2: 96 - 110. China's HIV Crisis on JSTOR (Accessed on 21 November 2024.) https://doi.org/10.2307/20033087

Guimarães, M.L., B.C.L. Marques, N. Bertoni, S.L.M. Teixeira, M.G. Morgado & F.I. Bastos 2015. Assessing the HIV-1 Epidemic in Brazilian Drug

Users: A Molecular Epidemiology Approach. *Brazilian Multicity Study Group on Drug Misuse* 10: 11: e0141372. https://doi.org/10.1371/journal.pone.0141372. (Accessed on 29 November 2024.) https://doi.org/10.1371/journal.pone.0141372 PMid:26536040 PMCid:PMC4633026

Hellman, M. 2022. *Drug Control and Human Rights in the Russian Federation*. Drug control and human rights in the Russian Federation - PubMed. https://doi.org/10.1177/14550725221108789 PMid:36003121 PMCid:PMC9379298

Jha, B. 2022. Drug Trafficking: A Critical Analysis. *Indian Journal of Law and Legal Research* 3,2: 1-18. Drug Trafficking: A Critical Analysis (Accessed on 22 November 2024.)

Kriegler, February 2023. *A Drug Policy and its Economic Cost: An Overview of Law Enforcement and Social Costs in Eastern and Southern Africa*. The Eastern and Southern Africa Commission on Drugs. Anine-Kriegler-Drug-policy-economic-cost-An-overview-of-law-enforcement-and-social-costs-in-Eastern-and-Southern-Africa-GI-TOC-February-2023.pdf

Levac, D., H. Colquhoun & K.K. O'Brien 2022. Scoping Studies: Advancing the Methodology. *Implementation Science* 5: 1 - 9. https://doi.org/10.1186/1748-5908-5-69 PMid:20854677

Levitsky, M. 1992. Drug Trafficking in China. *US Department of State Dispatch* 3, 21: 415-417. Law Journal Library - HeinOnline.org (Accessed on 25 November 2024.)

Lipton, D.S. 1997. HIV/AIDS, Drug Abuse Treatment, and the Correctional System. *Journal of Offender Rehabilitation* 25, 3-4: 19 - 34. Law Journal Library - HeinOnline.org (Accessed on 22 November 2024.) https://doi.org/10.1300/J076v25n03_02

Lunze, K., D. Lioznov, D.M. Cheng, R.V. Nikitin, S.M. Coleman, C. Bridden, E. Blokhina, E. Krupitsky & J.H. Samet 2017. HIV Stigma and Substance Abuse among HIV Positive Russians with Risky Drinking. *AIDS and Behaviour*. HIV Stigma and Unhealthy Alcohol Use Among People Living with HIV in Russia - PMC (Accessed on 23 November 2024.) https://doi.org/10.1007/s10461-017-1820-8

Eastern and Southern Africa Commission on Drugs, August 2023. *Maritime-based Drug Trafficking in Eastern and Southern Africa – An Overview.* Maritime-based-drug-trafficking-in-Eastern-and-Southern-Africa-An-overview-GI-TOC-August-2023.pdf (Accessed on 20 November 2024.)

Martens T. 2024. How Drugs and Alcohol can Fuel Violent Behaviours. *American Addiction Centres.* https://americanaddictioncentres.org (Accessed on 27 November 2024.)

Meng, J. 2016. The Legal Challenges to HIV in China. *Journal of Comparative Law* 11, 2: 153 - 165. Law Journal Library - HeinOnline.org (Accessed on 23 November 2024.)

Michels,I.I., Y.X. Fang, D. Zhao, L.Y. Zhao & L. Lu 2007. Comparison of Drug Abuse in German and China. *Acta Pharmacologica Sinica* 10: 1505 - 1518. Comparison of drug abuse in Germany and China - PMC (Accessed on 20 November 2024.) https://doi.org/10.1111/j.1745-7254.2007.00633.x

Mitra, P. 2004. India at the Crossroads: Battling the HIV/AIDS Pandemic. *Washington Quarterly* 27, 4: 95 - 110. Law Journal Library - HeinOnline.org (Accessed on 20 November 2024.) https://doi.org/10.1162/wash.2004.27.4.95

Pachuau, L.N., C. Tannous, M.V. Dhami *et al.* 2022. HIV among People Who Inject Drugs in India: A Systematic Review. *BMC Public Health* 22, 1529. https://doi.org/10.1186/s12889-022-13922-2 (UNAIDS; HIV and people who use drugs 2021.) (Accessed on 25 November 2024.) PMid:35948967 PMCid:PMC9367073

Parry, C., P. Petersen, T. Carney, S. Dewing & R. Needle 2008. Rapid Assessment of Drug Use and Sexual HIV Risk Patterns among Vulnerable Drug Using Populations in Cape Town, Durban and Pretoria. *Journal des Aspects Sociaux du VIH/SIDA* 5, 3:113 - 119. Rapid assessment of drug use and sexual HIV risk patterns among vulnerable drug-using populations in Cape Town, Durban and Pretoria, South Africa - PubMed (Accessed on 25 November 2024.) https://doi.org/10.1080/17290376.2008.9724909

Patel, R.M. 2023. Drug Abuse and Addiction: Analysing its Causes, Consequences and Legal Provision in India. *International Journal of Law Management & Humanities* 6: 3372 - 3382. Law Journal Library - HeinOnline.org (Accessed on 22 November 2024.)

Patil, K. & A. Pandey 2022. Drug Trafficking: A Growing Problem for India. *Asian Journal of Forensic Sciences* 1,1: 34 - 41. https://www.researchgate.net/profile/Ketan-Patil-5/publication/358279496_Drug_Trafficking_A_Growing_Problem_for_India/links/61fa9de01e98d168d7e7d8f1/Drug-Trafficking-A-Growing-Problem-for-India.pdf

Perrenoud, L.K.F., A.V. Oikawa, R. Williams, B. Laranjeira, J. Fischer, J. Strang & M. Ribeiro, April 2021. Factors Associated with Crack Cocaine

Early Initiation: A Brazilian Multicentre Study. BMC Public Health. A Public Health Crisis. Factors associated with crack-cocaine early initiation: a Brazilian multicenter study | BMC Public Health | Full Text https://doi.org/10.21203/rs.3.rs-62962/v1

Proinde, 30 July 2023. Update on Maritime Cocaine and Trafficking in Brazil. https://proinde.com.br/news/update-on-maritime-cocaine-trafficking-in-brazil/ (Accessed on 21 November 2024.)

Saah, T. 2005. The Evolutionary Origins and Significance of Drug Addiction. *Harm Reduction Journal* 2:8. www.harmreductionjournal.com/content/2/1/8 (Accessed on 23 November 2024.) https://doi.org/10.1186/1477-7517-2-8

SAPS 2024. Crime Statistics 2023/2024. South African Police Service Services | SAPS (South African Police Service)

Shereda, J. 1998. The Internationalization of the War on Drugs and Its Potential for Successfully Addressing Drug Trafficking and Related Crimes in South Africa. *George Washington Journal of International Law & Economy* 31: 297 - 298. Law Journal Library - HeinOnline.org (Accessed on 25 November 2024.)

Singer, M. 2006. Drugs and Development: The Global Impact of Drug Use and Trafficking on Social and Economic Development. *International Journal of Drug Policy* 19, 467 - 478. Drugs and development: the global impact of drug use and trafficking on social and economic development - PubMed. https://doi.org/10.1016/j.drugpo.2006.12.007 PMid:19038724

Singh, D. & M. van Zyl 2007. South Africa: An Opportunistic Narcoscape for International Drug Trading. *Acta Criminologica* 20, 1: 123 - 143. South Africa: An Opportunistic Narcoscape for International Drug Trading | Office of Justice Programs (Accessed on 27 November 2024.)

The Globalist 2024. BRICS v G7 GDP Comparison. www.thegloabalist.com

UNAIDS 2021. Global HIV and AIDS Statistics. United Nations

UNODC 2023. World Drug Day Report 2023. United Nations Office on Drugs and Crime.

United Nations Office on Drugs and Crime (UNODC) 2024a. The *World Drug Report 2024: Key Findings and Conclusions.* World Drug Report 2024 (Accessed on 29 November 2024.)

United Nations Office on Drugs and Crime (UNODC) 2024b. The *World Drug Report 2024: Special Points of Interest.* World Drug Report 2024 - Special Points of Interest (Accessed on 29 November 2024.)

United Nations Office on Drugs and Crime (UNODC) 2024c. The *World Drug Report 2024: Contemporary Issues on Drugs.* unodc.org/documents/data-and- analysis/WDR_2024/WDR24_Contemporary_issues.pdf (Accessed on 29 November 2024.)

Wani, A. S. Patil 2024. The Narcoterrorism Challenge to India's National Security. https://www.orfonline.org/research/the-narcoterrorism-challenge-to-india-s-national-security

Wodak, A. 1998. Health, HIV Infection, Human Rights, and Injecting Drug Use. *Health and Human Rights* 2, 4: 24 - 41. Law Journal Library - HeinOnline.org (Accessed on 23 November 2024.) https://doi.org/10.2307/4065185 PMid:10347366

2025. *White House Memorandum on the Presidential Determination on Major Drug Transit or Major Illicit Drug Producing Countries for Fiscal Year 2025*. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/09/15/memorandum-on-the-presidential-determination-on-major-drug-transit-or-major-illicit-drug-producing-countries-for-fiscal-year-2025/ (Accessed on 25 November 2024.)

Yang, J. & M. Giummarra 2021. Compulsory and Voluntary Drug Treatment Models in China: A Need for Improved Evidence-based Policy and Practice to Reduce the Loaded Burden of Substance Use Disorders. *International Journal of Drug Policy* 92. Compulsory and voluntary drug treatment models in China: A need for improved evidence-based policy and practice to reduce the loaded burden of substance use disorders - PubMed (Accessed on 20 November 2024.) https://doi.org/10.1016/j.drugpo.2020.103063 PMid:33303344

Zanoni, B.C., C. Milford, K. Sithole, N. Mosery, M. Wilson, S. Bosman & J. Smit 2023. High Risk Injection Drug Use and Uptake of HIV Prevention and Treatment Services among People who Inject Drugs in KwaZulu-Natal, South Africa. *PLOS ONE* https://pmc.ncbi.nlm.nih.gov/articles (Accessed on 22 November 2024.) https://doi.org/10.1101/2023.01.16.23284613

Dr. Sandhya Maharaj
School of Law, College of Law and Management Studies
University of KwaZulu-Natal
(Attorney and Conveyancer of the High Court of South Africa)
Durban
MaharajS2@ukzn.ac.za

# Chapter 11: Cooperation in Countering Transnational Crime

**Nontyatyambo Pearl Dastile**
**ORCID iD: https://orcid.org/0000-0002-7903-9308**

> A new mindset is critical for keeping up, staying ahead, and countering transnational terrorism. It starts with each of us, in our respective roles and capacities (Thao & Dowler 2005).

## Abstract

The main thrust of this paper is a critical examination of the multifaceted domain of transnational crime, with a specific emphasis on strategies that hold promise for the mitigation and curtailment of such activities. This paper delves into the exigencies of forming countering strategies for addressing the pervasive issue of transnational transgressions. Structurally, the discourse is partitioned into four chronological segments, initially focusing on contextualizing the ensuing argument through John Burton's theoretical prism. The author explores proposed multi-stakeholder interventions before culminating in prescriptive recommendations advocating for the BRICS nations to forge symbiotic alliances with academic institutions and other entities, thereby facilitating sustainable solutions to the pervasive issue of transnational crime.

**Keywords:** Transnational crime, multi-stakeholder relations, BRICS, Human Needs Theory

## Introduction

The critical engagement in countering transnational crime commences with an assertion from Thao and Dowler (2005), articulating the indispensability of a refreshed mindset for the efficacious navigation and confrontation of transnational terrorism. Following this, the abstract elucidates the document's nucleus – the proposition of actionable intelligence and collaboration within the BRICS nations aimed at the attenuation of transnational criminal endeavors. Central to the treatise is the application of John Burton's human needs theory as a lens through which multi-stakeholder interventions' root causatives – denoted as push and pull factors – are analyzed. This theoretical framework facilitates a conscientious evaluation of both global strategies and cooperative mechanisms tailored to combat these pervasive crimes, assessing the evolutionary trends and impacts thereof. The literature review ardently champions the espousal of multi-stakeholder methodologies, emphasizing the limitations inherent in predominantly state-led initiatives, such as the lack of diverse perspectives and the potential for political bias.

Several complex factors have significantly impacted the rapid growth of transnational crime. These factors encompass a range of elements, including the permeability of borders, large-scale population movements, advancements in financial and commercial sectors, and the evolution of communication technologies (Makarenko 2001: 22). These influences have fundamentally transformed our understanding of transnational crime. It is worth noting that political systems and the deteriorating socio-economic conditions prevalent in various regions across the globe, including within the BRICS bloc, have played a crucial role in shaping the landscape of transnational crime. Unlike highly organized criminal activities, transnational crimes lack a rigid hierarchical structure and notably exhibit fluidity, which indicates that new members can be rapidly integrated into the leadership framework. In contrast, existing members can be easily replaced (Makarenko 2001).

Consequently, transnational crime has increasingly been recognized as a significant national and regional security threat. A pivotal aspect of this recognition is the enduring connection between criminal enterprises and terrorist factions, as indicated by Mararenko (2001). Efforts spearheaded by individual countries or state mechanisms have proven inadequate in addressing the challenges of transnational crime within the BRICS nations. This inadequacy has led to a continued escalation in criminal activities, exacerbated by the permeable frontiers of these countries. This situation has facilitated the

growth in acts of violent extremism, terrorism, and other offenses, which, although seemingly minor, have significantly undermined the capacity of these nations to engage in multi-stakeholder collaborations and enhance cooperation within the BRICS coalition.

Mwaniki (2019: 22) critically assesses the counter-terrorism strategies employed in Kenya, highlighting a reliance on militaristic approaches. He contends that such reliance on sheer force proves futile in scenarios where disenfranchised youth turn towards joining militant terrorist groups, thereby embracing the group's culture and violent practices. Once entrenched, this cycle of violence finds its way into various societal structures, including institutions of higher learning, places of worship, and commercial centers (Mwaniki 2019: 4). However, the strategies and multi-stakeholder initiatives proposed by the current discourse cannot be grounded in universal principles for countering transnational crime due to the unique economic landscapes of the BRICS member states. Notably, the existence of 'weak and impoverished states' poses a critical challenge by endangering the livelihoods of citizens, thus rendering them susceptible to exploitation by terrorist entities. This necessitates adopting counter-strategies tailored to each country's specific requirements and conditions (Patrick 2007: 645). The section below delves into the complexities associated with defining the term to develop more precise and sophisticated definitions that align with the strategic goals of BRICS.

## Conceptualising Transnational Culture

There are many different definitions of transnational crime, each encompassing a range of illegal activities such as drug trafficking, money laundering, terrorism, and pornography. Therefore, researchers need to consider how this concept is defined carefully. The variation in definitions from one country to another significantly impacts the conceptualization of transnational crime. The specific details and nature of these crimes must be considered when defining each country. Zabyelina (2010: 42) notes that definitions of transnational crime are often broad and all-encompassing, and the lack of clear boundaries and understanding of the severity of transnational crime further complicates matters. As a result, each country's definition is influenced by its unique position and characteristics. Therefore, an overarching definition that delves into the specific characteristics of each criminal activity falling under the umbrella of transnational crime is necessary.

The BRICS bloc member states must each contribute to identifying numerous criminal activities falling under the transnational crime category. Given the fluidity in the definition of this type of crime, these member states must strategize interventions to combat transnational crime. Therefore, any definition should be specific and meaningful, and discussions involving various stakeholders are imperative for rethinking and reconceptualizing the definition of transnational crime.

Zabylena (2020) discusses the challenge of defining transnational crime, noting that the United Nations has repeatedly attempted to establish a global definition since 1975. Despite these efforts, a precise definition has remained elusive. Renewed endeavors in 1994, under the Naples Political Declaration and Global Plan of Action, aimed to reach an internationally agreed-upon definition, with uncertain participation from BRICS bloc member states. Subsequent meetings and conventions, including those led by the United Nations Survey on Crime Trends and the United Nations Convention against Transnational Crime and its Protocols in 2010, highlighted key characteristics of transnational crime. According to Zabylena (2010), transnational crime is marked by systematic or occasional corruption and violence, the investment and manipulation of illicit goods and services, and the pursuit of high economic or socio-political benefits. Van Lampe (2012) also identified five ways to define transnational crime, focusing on aspects such as individual offenders, criminal activities, organized offender groups, and the geographical scope of transnational organized crime (Van Lampe 2012: 179).

The study identified certain advancements in addressing transnational crime. However, it is disappointing to note that some scholars have solely focused on individual offenders in transnational crime, with the field of criminology primarily concentrating on individual characteristics around 2012. Consequently, the conceptual definitions of transnational crime have remained under-researched. It is imperative for researchers delving into transnational crimes to recognize that such crimes cannot be scrutinized from a linear perspective. Albini and Mcllwain (2012) highlighted that ‘criminal groups are dynamic entities, not static ones, changing with the nature of the criminal acts they commit’. This illuminates the need for a more comprehensive understanding of transnational crime beyond individual traits.

The existing discussion on transnational crime reveals significant disparities and deficiencies in research within the discipline of criminology. Luong (2020) illustrates the stark contradictions in studying this crime within specific regions. Pineda (2022) advocates for ‘civil disobedience’ to confront

issues of poverty, violence, and statelessness, emphasizing that a nuanced understanding of the underlying issues is crucial in comprehending transnational crime. Limited knowledge of transnational crime within different countries, as mentioned by Luong (2020), may impede efforts to counter transnational organized groups. Ngor (2004) simplifies transnational organized crime as the movement of persons, goods, and services across national jurisdictions devoid of acceptable norms and standards. The following discussion focuses on the Human Needs Theory (John Burton) as one of the theoretical frameworks that may facilitate meaningful cooperation in countering transnational crime.

## John Burton's Human Needs Theory (HNT)

### *Human Needs and Crime*

In his 1979 publication, Burton highlights the enduring presence of unresolved political and social-political issues across various spheres of interaction, including family dynamics, educational environments, industrial settings, intercommunal relations, and international affairs. The persistence of wars, revolutions, and transnational crime on a global scale underscores the need for diverse approaches informed by the Human Need Theory (HNT), with tailored solutions required for each country.

Burton's Human Needs Theory (HNT) raises important issues regarding the failure of states to explore alternative frameworks for understanding human conflict. While many countries use broad labels such as terrorism to describe these conflicts, it is crucial to recognize that addressing conflict resolution should prioritize internal tensions that often spill across borders Burton (1979: 2. This emphasis is particularly relevant when examining transnational crime, which demands diverse and adaptable theories to explain its occurrence. The theory argues that when human needs are unmet, transnational crime becomes a viable means to an end for specific individuals. For instance, within the BRICS bloc, South Africa experiences high crime due partly to the government's failure to provide sufficient livelihoods. Therefore, Burton (1990) contends that HNT emphasizes the need for any study of transnational crime or conflict-affected nations to focus on understanding the fundamental human characteristics at play. In this light, Burton's HNT underscores the importance of acknowledging human involvement in all forms of criminal or conflict-related activity.

## *Contours of HNT*

The principle behind the concept of HNT is that 'human needs are fundamental motivations connected to personal advancement and well-being' Gallagher (2019: 23). These needs are inherent to all individuals and should be fulfilled regardless of their involvement in a particular country or community. To truly integrate individuals into a community, member states should define human needs by the resources available in the country. When these basic human needs are not acknowledged, many countries resort to excessively punitive measures and incarceration for individuals who break the law. However, these countries fail to realize that without meeting these fundamental human needs, individuals are more likely to turn to criminal behavior, leading to them being labeled as repeat offenders. It is important to note that discussions about human needs (HNT) should emphasize their emergent and non-hierarchical nature (Marker 2003). Human needs are diverse and specific to each country, as highlighted by scholars, academics, and civil rights organizations. Redekop (2002: 164) and Walsh (2016: 286) offer a comprehensive list of priority human needs, which includes safety, belongingness, love, self-esteem, personal fulfillment, identity, cultural security, distributive justice, participation, and freedom.

Griffiths (2013: 63) introduces another dimension: 'a need for control of one's respective environments and a need to have prospects'. Cook-Hoffman (2009: 22) asserts that human needs should be linked to 'issues of identity, including the ability to develop a collective identity, to have that identity recognized by others, and to have fair access to the systems and structures that support and define the conditions that allow for the achievement and building of identity'. Additionally, Burton in Scimecca (1990: 206 - 207) highlights specific needs such as consistency in response, stimulation, security, recognition, distributive justice, the appearance of rationality, meaningful responses, a sense of control, and a need to defend one's role. Fundamentally, various needs contribute to growth and development.

In her research, Gallagher (2019: 23) highlights the challenge of identifying these needs cohesively, potentially leading to missed opportunities for collaboration and multi-stakeholder relations with other countries. Nevertheless, Burton (1979) acknowledges that there may be commonalities among these needs while also recognizing their specificity and universal nature. Redekop (2002: 164-165) outlines specific met characteristics of human needs, including self-respect, self-esteem, self-confidence, self-recognition, and ultimately, self-actualization. Human needs theorists express concern that specific

ontological and genetic needs will persist regardless of socialization processes and that incompatible socialization can result in frustration Burton J. 1990b, pp. 33-34. In the face of persistent injustices, it should come as no surprise when individuals or groups turn to violence Schmid (2005).

Gallagher (2019:6) contends that discussing human needs must not be divorced from recognizing human identity. Human Needs Theory and Human Identity needs have become a significant motivator for specific ethnic communities. As noted by Wolff (2006: 31), '[A]s ethnicity [and identity] attain political significance, influencing the life opportunities of individuals from diverse ethnic backgrounds, it becomes plausible to mobilise group members to instigate change in contexts characterised by persistent discrimination and disadvantage. Alternatively, such dynamics may also serve to reinforce a valued *status quo*.

In order to effectively reduce the prevalence of transnational crimes, HNT must be integrated with conflict resolution in multi-stakeholder interventions Redekop (2022). Embracing multi-stakeholder interventions and HNT empowers researchers to employ diverse strategies in tackling transnational crime. This approach offers the benefit of exploring alternative methods and generating new insights.

As Cook-Hoffman (2009: 22) points out, using HNT enables scholars to comprehend various forms of violent social conflict more accurately, how it manifests, and potential changes to foster positive peace. Despite its pitfalls, HNT provides alternative knowledge that allows researchers to make predictions and consider different policy options. This underscores the importance of understanding how fulfilling basic human needs can mitigate transnational crime.

## *Critique of HNT*

The HNT model has received widespread recognition for its analytical simplicity; however, Reiman (2002) criticizes its failure to address gender-specific needs. Reiman suggests integrating gender-specific nuances and culture-sensitive approaches into the model to rectify this shortcoming. In some social science disciplines, there has been a tendency to overlook gender, resulting in the silencing of women and the erosion of their agency. Reiman's argument advocates for a multifaceted approach that highlights the visibility of gender-specific needs and encourages researchers and scholars to pose relevant questions rather than make assumptions about transnational crime's gendered

aspects. Arsovska and Allum (2014) express disappointment at the insufficient analysis of women's involvement in transnational crime. Despite the scarcity of gender-specific theoretical discussions, scholars should prioritize identifying and redressing gendered needs when revising the HNT model. While the model may lack nuances highlighted by some scholars, the model allows scholarship interventions that may be specific to address contemporary issues such as the scourge of transnational offending—regional analysis dovetailing into a global analysis enabling trans-disciplinary models to emerge in combating transnational crime. Such enables multi-disciplinary co-operations, as discussed below.

## Co-operation in Countering Transnational Crime

The collaboration of multi-stakeholder, multi-transdisciplinary approaches to address transnational crime poses ongoing challenges due to the continuously evolving tactics of offenders and the rapid advancement of technology. Offenders often exploit technological trends that many law enforcement personnel may not be fully familiar with. One example of such sophisticated criminal activity is cyberterrorism, where perpetrators steal through the manipulation of advanced computer systems using scams, forgeries, and counterfeit goods. Many law enforcement agencies lack personnel who are proficient in advanced technologies and computer literacy necessary to combat cyberterrorism effectively. Additionally, developing countries within the BRICS lack the resources to provide law enforcement agencies with the latest technologies to combat cybercrime, in part due to limited state budgets and a lack of political will compared to countries in the Global North.

While addressing this issue, it's important to consider a comprehensive approach. First, countries in the Global North should strengthen their legislation to penalize association with criminal groups and their affiliates. Second, investing in advanced techniques, such as improved surveillance and enhanced undercover operations, is crucial. The third step involves locating transnational gang members who can provide testimony in a court of law and reveal the identities of witnesses involved in transnational crime, with a focus on witness protection. Additionally, criminal law measures should be tightened globally to criminalize participation in transnational crime and address the challenge of offender mobility. To counteract the tendency of offenders to flee across borders, strict passport control measures should be implemented by BRICS country members. Collaboration between nations is essential to implement these strategies through multi-stakeholder interventions. Furthermore, both the

Global North and South should review and enforce their extradition laws and regulations to strengthen bilateral relations.

In a research study conducted by ARLEMP, Thao and Dowler (2005: np), participants acknowledged that operational outcomes will remain unchanged unless we modify our operational practices. They emphasized that continuing with the same law enforcement approaches will yield the same results. Participants unanimously agreed that it is imperative to shift our mindset regarding our understanding of terrorism, which will subsequently improve how we tackle the operational challenges posed by this constantly evolving form of crime. Without a comprehensive understanding of the scope of international terrorism, as well as the motivations, methods, and reach of terrorists, violent extremists, and foreign terrorist fighters in our countries, it becomes challenging to prevent and disrupt potential terrorist attacks effectively. As the literature synthesis in this paper is not exhaustive, the suggested recommendations call for collaborative engagements within the member states as interventions are deliberated.

## Recommendations for Network Collaborations within Sectors

Several collaborative initiatives have been suggested to address transnational crimes, with input from researchers and private organizations to the government. The discussions about these proposals, presented in a non-specific order, focus on how effective they could be within the BRICS (Brazil, Russia, India, China, and South Africa) bloc.

Transnational crime impacts all branches of government at the presidential level. Each member state's President must develop policy directives to engage multiple stakeholders. It is crucial for presidential candidates to review current policies and frameworks within government branches. This involves engaging members of parliament and all political parties in shaping enforcement models. This shift requires moving away from traditional policing and selective enforcement and utilizing change agents at the highest level of parliamentary structures. These change agents are crucial in identifying gaps in existing policies and enforcement initiatives, monitoring the revised strategy, and ensuring compliance. During the policy revision phase, it is essential to clearly outline the role of police-led interventions based on collaborations and treaties with other countries.

Countries must invest in highly qualified staff with relevant experience in each parliamentary body, particularly in intelligence-led interventions. As a result, countries lacking political will can consider other BRICS countries' initi-

atives during discussions at bodies such as the Pan African Parliament. Facilitating staff exchanges could enable the transfer of knowledge and skills to intelligence members within the BRICS. The level of engagement among the presidents of BRICS countries has become increasingly important, and the agenda on curbing transnational crime should be a standing item in high-level meetings.

It is advisable to permit multi-stakeholder partnerships, with at least one specified department overseeing identifying individuals involved in transnational crime. Depending on the organizational setups of BRICS parliaments, the governing body headed by the Minister should enhance identification measures to curtail criminal activities that often involve travel. The primary objective of this initiative is to disrupt criminal operations.

It is widely acknowledged that certain countries in the Global South may lack the necessary funding to support this initiative. One of the countries funded by the Global North must set an example for other developing nations. However, not all countries in the Global North have high levels of transnational crime. Collaborating with academics and private entities to conduct statistical analysis can help identify countries at high risk. A collective effort by multinational countries can facilitate the allocation of funds to the most affected countries through donor funding, establishing intelligence capabilities to combat transnational crimes. Moreover, facilitating staff exchanges within these countries can foster knowledge exchange and streamline interventions tailored to each country's needs.

Lawson and Bersin (2020) highlight the failure of countries to form partnerships to counter transnational crimes through border management. They point out that border porosity is a critical factor contributing to the proliferation of transnational crime. The authors also observe that 'Unilateral thinking impedes intelligent management of critical infrastructures such as pipelines or electricity grids, and natural resources such as water systems and habitats that span borders'. Despite policymakers' awareness of this issue, affected countries are hesitant to collaborate, even in the Global South.

The effectiveness of border management has a significant historical context. Many countries in the 19th century did not prioritize strengthening border management as a means to curb transnational crime. It was not until the end of the 19$^{th}$ century that initiatives were taken in Europe, but these interventions did not consider intelligence-led and multi-stakeholder involvement in border management. Instead, the main discussions revolved around deploying security personnel at the borders without adequate intelligence-led training to address porous borders.

As transnational crime increased, the need for bilateral partnerships became apparent, leading to developing strategies and policies to address border porosity and its role in escalating crimes. Government interventions and the use of highly trained operatives have been instrumental in reducing cross-border criminal activities. Progress can also be seen in some countries within the Global South, such as Nigeria and Niger.

Yakubu and Idehen (2021) discuss various forms of border management in these countries, highlighting the complexity of securing borders due to the complexity of the environment and the high volume of activities. Strategies used in Nigeria and Niger include surveillance, patrols, joint control operations, information exchange, and intelligence gathering and assessment. While efforts to revise and improve frameworks and policies are ongoing, they are hindered by the evolving nature of transnational crimes and the methods used by offenders to outpace state-led interventions. Allocating substantial budgets and resources, including providing high-tech training to border patrol officers, is critical to the success of these interventions. Moreover, a heavy reliance on risk management to analyze new trends must be supported by forming multi-strategies to gather intelligence from various sources, ultimately reducing unilateral intelligence-led interventions.

The erection of border walls in certain countries has profoundly affected interactions with neighboring communities. For example, the proposal to build walls between the US and Mexico during the previous administration was widely regarded as a divisive and racially charged move by many, including members of the Trump administration itself and Democratic officials. G7 leaders strongly condemned this approach and also drew dissatisfaction from some Global North countries despite the support it received from others.

An example of another country following a similar path is Saudi Arabia, which constructed the Great Wall under the guise of protecting itself from the terrorist group ISIS. However, it is crucial to emphasize the importance of involving local community structures. Community knowledge and intelligence are integral in identifying and monitoring potential offenders and their meeting places, which often go overlooked.

In a study by ARLEMP authors Thao and Dowler (2005), one participant highlighted the necessity of global collaboration in combating terrorism, stating, ‘One country cannot solve terrorism alone, so we need to work together and understand each other’s cases, risks, and actions.’ The survey participants concluded that breaking networks involved in criminal activities requires a network of cooperation. This emphasizes the critical need for high-level colla-

boration between law enforcement, citizens, and non-profit organizations. However, it was also recognized that the political and community sensitivities present significant challenges to such collaboration.

Intelligence-sharing is crucial in this collaborative effort, yet it faces the obstacle of secrecy prevalent in law enforcement agencies. Breaking down these barriers by fostering transparency and sharing intelligence is essential. Thao (2021) emphasizes the importance of 'Dare to Share' as a valuable lesson for everyone. She highlights our critical role in contributing to the intelligence map and acknowledges the limitations of messaging applications for certain types of information. She asserts the readiness to share and emphasizes the need for robust systems to promptly and securely convey intelligence information. Thao encourages continued dialogue on this crucial matter.

## Proactive Investigative Approaches

It is crucial to allocate a sufficient budget to intelligence cooperatives for this approach to be practical. This will require proactive strategies that depart from traditional investigation methods Thao and Dowler (2005: np). By prioritizing improved investigative capabilities and prosecution techniques within states, mechanisms to combat transnational crime can be enhanced. Sharing these strategies with other countries is essential to promote proactive vigilance and early detection of transnational criminal activities. Therefore, it is imperative to bolster community cooperation, which can be achieved through civilian involvement, as police-led intelligence efforts alone are insufficient without civilian participation. Thao and Downer (2005) emphasize that law enforcement cannot tackle justice pursuits in isolation, especially in terrorism cases. They stress the importance of engaging the community in sharing vital intelligence. Consequently, practical police cooperation should encompass collaboration with government agencies, private sector entities, academia, media, and the broader community.

Community involvement can be encouraged through various means, including compensation and incentives to ensure confidentiality and anonymity. Protecting law enforcement and confident community members for all volunteers working to combat transnational crime is crucial. Although these approaches may be practical, it is essential to emphasize the proactive nature of global networks engaged in transnational crime and the need for offense classifications that prioritize these crimes.

## Conclusion

The introductory discourse posits various catalysts augmenting the proliferation of transnational crime, explicitly referencing border porosity, technological advancements, and deteriorating socio-economic conditions within the BRICS realm as pivotal elements. The narrative advances by delineating the non-hierarchical structure peculiar to transnational crimes, illustrating their dynamic nature and the ease of recruitment and replacement within their ranks. This seminal piece attributes the escalation of national and regional security threats to the intricate nexus between organized criminal entities and terrorist factions, and underscores the crucial role of the BRICS nations in countering transnational crime.

Reflecting on the inadequacies of state-centered interventions, the author illuminates the continual expansion of transnational criminal activities exacerbated by ineffective border controls. The critique extends to the military-centric counter-terrorism measures employed, exemplified by Kenya's approach, which sporadically engenders counterproductive outcomes. The groundwork is laid for a nuanced understanding that eschews a one-size-fits-all mentality in favor of localized, country-specific strategies, particularly in regions where state fragility facilitates the exploitation of vulnerable demographics by terrorist operatives.

Recommendations are made for the BRICS bloc member states to prevent transnational crime from thriving due to a lack of political will. The Global South will only attract donor funding if it strengthens its country's initiatives to attract foreign investments. To effectively combat transnational crime, all countries must develop comprehensive definitions based on shared visions and goals. Academics and scholars should play a key role in providing long-lasting conceptual definitions of transnational crime adapted to each country. It is imperative for various stakeholders, including community members, scholars, police, and internal collaborators, to share insights and conceptualize solutions. Therefore, further research should focus on each offense categorized as a transnational crime to identify synergies in combating these crimes and finding long-term solutions. All stakeholders need to come together to address the loss of life resulting from these crimes.

## References

Albini, J.L. & J.S. McIllwain 2012. *Deconstructing Organized Crime: A Historical and Theoretical Study*. McFarland.

Arsovska, J. & F. Allum 2014. Introduction: Women and Transnational Organized Crime. *Trends in Organized Crime* 17: 1 - 15. https://doi.org/10.1007/s12117-014-9223-y

Burton, J. 1990. *Conflict: Human Needs Theory*. Cham, Switzerland: Springer. https://doi.org/10.1007/978-1-349-21000-8

Burton, J. 1997. *Violence Explained*. Manchester University Press.

Burton, J.W. 1979. *Deviance Terrorism & War: The Process of Solving Unsolved Social and Political Problems*. Australian National University Press.

Burton, J.W. 1979. *Deviance, Terrorism & War: The Process of Solving Unsolved Social and Political Problems*. Australian National University Press.

Cook-Hoffman, C. 2009. The Role of Identity in Conflict. In Sandole, D.J., S. Byrne, I. Sandole Staroste & J. Senehi (eds.): *Handbook of Conflict Analysis and Resolution.* London & New York: Routledge.

Dimou, E. 2021. Decolonizing Southern Criminology: What can the 'decolonial option' Tell us about Challenging the Modern/ Colonial Foundations of Criminology? *Critical Criminology 29*: 431 - 450. https://doi.org/10.1007/s10612-021-09579-9

Gagnon, J.P. & E. Beausoleil 2022. Editorial. *Democratic Theory* 9,1: 5 - 7. https://doi.org/10.3167/dt.2022.090101

Gallagher, S. 2019. *China's Repression of the Xinjiang Uyghur: Ethnic Conflict in Xinjiang, China and the Application of John Burton's Human Needs Theory*. Doctoral dissertation, Université Saint-Paul/ Saint Paul University.

Griffiths, M. 2013. John Burton versus International Relations: The Cost of Criticism. *Australian Journal of International Affairs* 67,1: 55 - 70. https://doi.org/10.1007/s10612-021-09579-9

Kar, D. & J. Spanjers 2017. Transnational Crime and the Developing World. *Global Financial Integrity* 53 - 59.

Lawson, C. & A. Bersin 2020. Collaborative Border Management. W*orld Customs Journal* 14:1. https://doi.org/10.55596/001c.116307

Luong H.T. 2020. Transnational Crime and its Trends in South-East Asia: A Detailed Narrative in Vietnam. *International Journal for Crime, Justice and Social Democracy* 9,2: 88 - 101.

https://doi.org/10.5(204/ijcjsd.v9i2.1147

Makarenko, T.2001. Transnational Crime and its Evolving Links to Terrorism and Instability. *Janes Intelligence Review* 13,11: 22 - 24.

Marker, S., August 2003. Unmet Human Needs. Beyond Intractability. http://www.beyondintractability.org/essay/human-needs

Mwaniki, D.M. 2019. *Changing Strategies in Countering Violent Extremism and Terrorism in Africa: Case of Kenya*. Doctoral dissertation, University of Nairobi.

NgorNgor, A.D. 2004. Effective Methods to Combat Transnational Organised Crime in Criminal Justice Processes: The Nigerian Perspective. *Resource Material Series* 58: 171 - 182.

Patrick, S. 2007. 'Failed' States and Global Security: Empirical Questions and Policy Dilemmas. *International Studies Review* 9,4: 644 -662. https://doi.org/10.1111/j.1468-2486.2007.00728.x

Redekop, V.N. 2002. *From Violence to Blessing.* Novalis.

Reimann, C. 2002. 'All You Need is Love' - and What about Gender? Engendering Burton's Human Needs Theory. Bradford, Centre for Conflict Resolution, Department of Peace Studies, University of Bradford. CCR Working Papers: No. 10. https://bradscholars.brad.ac.uk/server/api/core/bitstreams/2ae39994-5b58-4537-9380-061d9de179ee/content

Schmid, A.P. 2005. Prevention of Terrorism: Towards a Multi-pronged Approach. In Bjorgo, T. (ed.): *Root Causes of Terrorism: Myths, Reality, and Ways Forward.* London & New York: Routledge. https://doi.org/10.4324/9780203337653_chapter_18

Scimecca, J.A. 1990. Self-reflexivity and Freedom: Toward a Prescriptive Theory of Conflict Resolution. In Burton, J. (ed.): *Conflict: Human Needs Theory*. London: The Macmillan Press Ltd. https://doi.org/10.1007/978-1-349-21000-8_10

Sharoni, S. & J. Welland 2016. Introduction: Revisiting the Relationship between Gender and War: Reflections on Theory, Research, Activism, and Policy. In Sharoni, S., J. Welland, L. Steiner & J. Pederson (eds.): *Handbook on Gender and War*. Edward Elgar Publishing, Inc. https://doi.org/10.4337/9781849808927.00006

Steinmeyer, J.K. 2017. *An Examination of John Burton's Method of Conflict Resolution and Its Applicability to the Israeli - Palestinian Conflict.* The University of South Florida, Department of Philosophy. University of South Florida Scholars Commons.

Thao, N.P. 2021. Interview conducted on 26 June 2021.
Thao, N.P. & K. Dowler 2018. A New Mindset for Countering Transnational Terrorism. *Journal for Indo-Pacific Affairs* 1,1, Fall.
Von Lampe, K.2012. Transnational Organised Crime Challenges for Future Research. *Crime, Law and Social Change* 58: 179 - 194. https://doi.org/10.1007/s10611-012-9377-y
Zabyelina, Y. 2010. Unpacking Pandora's Box: Defining Transnational Crime and Outlining Emerging Criminal Trends. *Central European Journal of International & Security Studies* 4,2: 124 - 139.

Professor Nontyatyambo Pearl Dastile
Department of Social Sciences
Faculty of Law, Humanities and Social Sciences
Walter Sisulu University
Mthatha
ndastile@wsu.ac.za

# Chapter 12: Youth Unemployment and the Threat to Peace and Security: The Case of South Africa

**Shanya Reuben**
**ORCID iD: https://orcid.org/0000-0001-7922-9171**

**Shaida Bobat**
**ORCID iD: https://orcid.org/0000-0002-5199-5234**

## Abstract

South Africa's chronic and critically high rate of unemployment, particularly among youth, is cementing the country in a state of political, economic and social vulnerability. As one of the largest and most industrialised economies in Africa, it is perplexing that South Africa holds the highest level of youth unemployment in the continent. Notwithstanding South Africa's robust legal frameworks and sustained job-creation policy initiatives which arguably hold much promise for dealing with youth unemployment, our analysis suggests that efforts to date lack a holistic, consolidated approach to meaningfully resolving the issue of youth unemployment, the consequences of which threaten national and human security. This research adopts a literature review methodological approach and presents a synthesised narrative review on the current evidence and knowledge bases in the context of South Africa's youth unemployment. The overarching purpose of this literature review is to provide an overview of the multifaceted nature of youth unemployment in South Africa including the root cause, implications for national peace and security as well as an evaluation of the current strategies employed in tackling youth unemployment. Based on our analysis, we highlight the persistent challenge of South Africa's youth unemployment which pose significant political, economic and social threats to the nation. We provide some insights into potential pathways for dealing with South Africa's youth unemployment crisis, emphasizing in particular, a call for

a unified, coordinated national strategy to maximise efforts in addressing youth unemployment.

**Keywords:** Youth Unemployment, Peace and Security, BRICS, South Africa

## Introduction

Unemployment is a global concern. The ILO defines persons in unemployment as the condition in which 'those of working age who were not in employment, carried out activities to seek employment during a specified recent period and were currently available to take up employment given a job opportunity' (ICLS 2023: 14). The International Labour Organisation (ILO) suggests that current workplace conditions are compounded by falling living standards, weak productivity and persistent inflation, have induced conditions for greater inequality, and are undermining efforts to achieve social justice (ILO 2024). With approximately 402 million people estimated to be unemployed globally (ILO 2024) unemployment has been ranked 27 out of a total of 34 in terms of the most severe global risks we may face over the next decade (Global Risks Report 2024). Of note, while regions including North America, Europe, Japan, Canada, Australia and the United Kingdom continue to sustain relatively low rates of total population unemployment (ranging between 2.4% and 6.3%), BRICS nations report significantly higher levels of total population unemployment which range between 4% and 33% (Statista 2024).

Youth remain disproportionately impacted by unemployment with global estimates indicating 65 million youth are unemployed (World Economic Forum 2024). Similar to unemployment rates across total populations, regions including North America, Europe and Australia report lower youth unemployment rates which range between 10.4% and 16.3%. This is in stark contrast to BRICS nations where youth unemployment estimates reflect rates of 24.4% in Brazil, 23.3% in India, 15.3% in China 20.1% in Russia and, most concerning, 59.6% in South Africa (Statista 2024).

Noting the estimated youth unemployment of 59.6% (among the highest globally) in South Africa, we agree with the analysis of demography experts who note that youth suffer most in the context of critically high unemployment (World Economic Forum 2024). It is no wonder then that Molobela (2023) refers to unemployment as one of the most appalling socio-

economic issues in South Africa. The persistent challenge of youth unemployment has pushed South Africa's economic development into a downward spiral toward underdevelopment and vulnerability (Monama 2024) which, as opined by Lebakeng (2024), generates an unease about the future of youth, provoking anger towards society and government, increasing the risk of revolts which, when taken together, 'threaten state, national and human security' (p. 1).

Notwithstanding South Africa's robust legal frameworks and sustained job-creation policy initiatives which arguably hold much promise for dealing with youth unemployment (discussed later in this chapter), our analysis suggests that efforts lack a holistic, consolidated approach to meaningfully resolving (at least to some extent) the issue of youth unemployment. Our analysis, discussed in greater detail later in this chapter, considers the various causes of South Africa's high rate of youth unemployment including, for example, skills mismatches, an inadequate education system, stagnated economic growth and sustained social and political vulnerability. At the same time, we note the various calls for targeted strategies and intellectual frameworks for addressing youth unemployment including for example, accelerated entrepreneurship initiatives, skills development initiatives, governmental reforms, and coordinated responses involving key stakeholders. Noting both current vulnerabilities and calls for more fit-for-purpose strategies and frameworks to tackling South Africa's youth unemployment problems, we find merit focusing on the case of South Africa. We argue, given South Africa's unique historical landscape, ongoing inequality, and the implications of youth unemployment on social and economic stability, youth unemployment poses significant risks to peace and security in the country. We advance that prioritising sharper focus on South Africa's youth unemployment problems will not only contribute to the nation's economic growth but importantly, can provide frameworks and strategies for achieving a more inclusive, peaceful and stable society. Against this backdrop, we provide a brief summary of the approach informing the research in the next section.

## Research Approach

This research adopts a literature review methodological approach and presents a synthesised narrative review on the current evidence and knowledge bases in the context of South Africa's youth unemployment. Snyder (2019) describes literature review approaches as a basis for knowledge development, creating guidelines for policy and practice, and, when well executed, literature reviews

hold the capacity to present novel ideas and directions in a particular field. Similarly, Webster and Watson (2002) describe literature review methodologies as a good option for creating a foundation for advancing knowledge and theory development. A literature review approach was found appropriate for the purpose of the current study in that it provided a basis to access and map current evidence and knowledge states, and, at the same time, provide insights into better informing evidence-based policy and practice (Angioi & Hiller 2023).

Literature review designs may include research purpose framing, protocol development, and the identification, analysis and synthesis of data reflected in a narrative report (Parker & Sikora 2022). The purpose of this literature review was to provide a narrative overview of youth unemployment in South Africa including the root cause, implications for national peace and security as well as an evaluation of the current strategies employed in tackling youth unemployment. Data was sourced from various research databases and online platforms including PsycINFO, Google Scholar, Scopus, ProQuest, Sage Journals and Taylor & Francis Online, national statistics agencies, government reports, and news articles. Relevant data was themed and critically appraised. This review is novel in that key themes have been organised and presented into distinct topical sections, each of which reflect broader trends apparent from the data. As such, this narrative review reflects an organised discussion which contextualises and integrates key findings from the literature reviewed. The following distinct sections were informed by a critical review of literature, each of which is presented in turn: Youth Unemployment in South Africa; Factors Compounding Youth Unemployment in South Africa; the Nexus between Youth Unemployment and Threats to Peace and Security; Strategies Aimed as Reducing Youth Unemployment, and Future Directions.

## Youth Unemployment in South Africa

South Africa's unemployment crisis is complex, shaped by the country's history of apartheid, which was characterised by a racially based system of privilege. Under apartheid, the majority of the population remained politically, economically and socially disadvantaged. The educational and occupational marginalization among black South Africans enforced during apartheid (Treiman 2005), continue to reflect the legacies of apartheid where, despite 30 years into democracy, unequal access to land, education, employment opportunities among black South Africans, and in particular, the youth, abound (Klug 2024).

The centrality of work in people's lives, especially young individuals, is a significant factor and is one of the central motivators for identity construction (Martela & Pessi 2018). Employed youth are more likely to experience autonomy and meaningful social integration (Frias *et al.* 2020), develop prosocial identities (Oswald 2022) and be better positioned to connect and engage with social capital networks (McMurphy *et al.* 2019). We therefore agree with the suggestions outlined in the 2024 United Nations Development Programme Report that employment 'fosters human dignity, empowering individuals to develop their agency and skills, and equipping them with the means to shape their lives and contribute positively to their communi-ties'. Employed youth are a central precursor for national success.

Conversely, unemployed youth are more likely to experience stress, lower self-worth, anxiety and low self-esteem (Monama *et al.* 2024). Unemployment, particularly of young people (15 to 34 years of age), remains an enduring problem in South Africa. Youth, often viewed as a vehicle for future economic growth and innovation, now increasingly find themselves excluded from the economic mainstream, the implications of which are dire at both the individual and societal level. Munyati 2024) reports that the common element for social fragility within sub–Saharan Africa relates to a restless youth population with insufficient economic opportunities. Various perception surveys have consistently shown that many youth report feeling anxious about the economy, job stability, lack of social mobility and job loss (ILO 2024). It is not surprising then that youth report feelings of exclusion, alienation, and resentment, which, as opined by Pasara & Dunga 2022) fosters an environment of social and political turmoil (Pasara & Dunga 2022).

Habiyaremye *et al.* (2022) deduction is noteworthy with their suggestion that despite decades of policy initiatives to increase job readiness and employment opportunities for young job seekers, youth unemployment remains the Achilles' heel for most African economies. This is especially true in the context of South Africa where the persistent issue of youth unemployment is seemingly intractable. The unemployment rate among South African youth (aged 15 to 34 years) is alarming. 2024 youth unemployment rates ranged from 32.9% in Quarter 1, to 33.5% in Quarter 2, and currently stands at 32.1% in in the third quarter of 2024 (Statistics South Africa 2024). As one of the largest and most industrialised economies in Africa, it is perplexing that South Africa holds the highest level of youth unemployment in the continent. This context explains why Smith, in a 2023 *New York Times* article draws on South Africa's

Freedom Charter principles promulgating the 'right and duty of all to work', highlighting the unmet expectations of youth aiming for better prospects than their parents and grandparents. We ask the same question as Lannoy *et al.* (2020), 'Why is youth unemployment so intractable in South Africa?'. We offer some responses to this question later in this chapter. We first however turn our attention to the factors compounding youth unemployment in South Africa.

## Factors Compounding Youth Unemployment in South Africa

While BRICS nations continue to face challenges in dealing with youth unemployment, various successes have been noted. For example, Brazil's *First Employment Program* has been successful in improving youth employment rates (Costa & Santos 2021). In India, various programmes such as *Skills India* which promote vocational training and entrepreneurship have increased youth employment rates (Bhattacharya 2019). Similarly, Russia's *Youth Labour Exchange Programme* has also shown promise in reducing youth unemployment rates (Ivanov & Motozov 2020). Unfortunately, despite significant successes among most BRICS nations, South African youth continue to experience the highest rates of youth unemployed, currently estimated at 59.6% (Statistics 2024). Against this backdrop, we offer some analysis into the possible reasons compounding youth unemployment in South Africa.

The high unemployment rate in South Africa is a complex issue rooted in historical and structural factors. Among these is the well-known 'skills mismatch' factor, which describes the excess demand for skilled labour that prevails in a labour market characterised by the oversupply of unskilled labour. This legacy of apartheid has its roots in an educational system that was designed to deprive the disenfranchised majority of skills training. There has been ineffective implementation of the policy initiatives which have been introduced to address skills development despite the political transformation in 1994. Moreover, South Africa's unemployment malaise has deepened as a result of stifled job creation in an economy beset by long-run, low growth. The National Planning Commission's (NPC) diagnostic overview in 2010 emphasised the role of inadequate economic growth as a major cause of unemployment. This observation remains just as true in present times as high rates of unemployment persist in an abysmal growth environment that accentuates inequality and poverty levels (Allen *et al.* 2021). To make matters worse, South Africa's unemployment rates are vulnerable to economic shocks (Dadam & Viegi 2023).

For example, the effects of the Great Recession following the 2008 financial crisis and the COVID-19 pandemic had long-lasting effects on unemployment.

Youth unemployment is affected adversely by additional causes than just the structural factors discussed above. The youth unemployment rate is the percentage of people aged 15–34 who are looking for work but are not currently employed. The level of youth unemployment is alarmingly disproportionate in comparison to the official national rate. As of the third quarter of 2024, the official youth unemployment rate in South Africa was 45.5%. This rate is in stark contrast to the official national unemployment rate which was 32.9% in the first quarter of 2024 (Statistics South Africa 2024).

Many researchers have provided clear evidence that the employment prospects of youth improve with higher levels of education (Mlatsheni & Ranchhod 2017; Jubane 2021). However, despite some progress made, the South African schooling system remains dysfunctional, and the quality of education is poor. The Basic Education system's inadequate delivery of skills development is evident in the performance of learners. In an international assessment of the performance among grade 5 and 9 learners in mathematics and science involving approximately 50 countries, South Africa's grade 5 learners were ranked last in both mathematics and science, while grade 9 learners were ranked fifth-last for mathematics and second-last for science (Department of Basic Education 2024). These results are supported by the Department of Basic Education's assessment of learner's performance. The performance of 85% of grade 9 learners fell below the department's minimum standard for mathematics and 33% did not achieve the minimum standard for reading. (Department of Basic Education 2024; South African Systemic Evaluation 2022). Consequently, these learners will enter the labour market with sub-standard skills that do not meet the requirements of most jobs. Clearly the quality of teaching and learning in the basic education system is wholly inadequate and fails to assist in reducing unemployment.

There is evidence that disillusionment with an ailing schooling system contributes to startling dropout rates, with approximately 50% of learners failing to complete grade 12. De Lannoy and Swartz (2015) and Botha *et al.* (2023) attribute this attrition to poor quality teaching and learning, teacher absenteeism, lack of resources and school violence. Additional factors include financial constraints, the need to work, grade repetition and teenage pregnancy. (Branson *et al.* 2014; Mbongwa *et al.* 2024). Moreover, the TVET system has not been able to achieve its objective of providing an alternative avenue for

skills development opportunities for unmatriculated school leavers. Policies designed to enable those learners who leave school after grade 9 to enter the TVET system have been blunted, in practice, by many colleges restricting admission to matriculants only. (Branson *et al.* 2015). Consequently, many of those who drop out of school will not have the skills to gain employment.

Given that there are better prospects of employment after obtaining higher education qualifications, it's not surprising that there were 1 068 046 students enrolled in HEI in 2021 (Department of Higher Education and Training 2023). However, recent statistics show that while large numbers of students aspire to gain a university education, a very large proportion of university entrants do not graduate. It has been reported that 38% of students in HEI, excluding UNISA, who enrolled for the first year of a 3-year undergraduate degree in 2016 had dropped out by 2021, and 62% graduated (Council on Higher Education [CHE] 2021). A dropout rate of approximately 40% is exceptionally high and suggests significant structural barriers to utilizing university education as a pathway to employment in South Africa, in contrast to patterns observed in other contexts. Factors that cause such a high dropout rate include financial constraints that affect the affordability of fees and other costs, inadequate basic education that leaves students underprepared for university and inadequate access to information such as career guidance at school (Branson *et al.* 2015; Kocsis & Molnár 2024). For the labour market, poor throughput in higher education affects the supply of high-level, skilled graduates.

There is a general consensus in the literature that tertiary education still provides some protection against unemployment in that it improves prospects for labour market participation. The evolving labour market, driven by the Fourth Industrial Revolution (4IR), demands skills such as digital literacy, communication, critical thinking, collaborative problem-solving, innovation, and self-learning. However, South African higher education institutions and TVET colleges have struggled to effectively equip students with these essential competencies (Onyilo *et al.* 2020) and the necessary soft skills that play a critical role in employability across various sectors, including both high- and low-skilled jobs. In lower-wage occupations, such as those in service work, soft skills are essential for effective performance (World Economic Forum 2023. These shortcomings combine to contribute to the misalignment between graduate qualifications and labour market needs and, consequently, unemployment. (HEPI 2023.

## The Nexus between Youth Unemployment and Threats to Peace and Security

Chido Munyati (Head of Regional Agenda, Africa, World Economic Forum) issues a stark warning that if jobs are not quickly created '… there is an increased risk that disaffected youth could become a source of instability in already fragile societies' (2024: 3). Economists and academics make compelling arguments on the relationship between high unemployment and the associated costs to individuals and society. Employment is championed as a catalyst for economic stability, social security and cohesion and peacebuilding. Conversely, the ramification of high unemployment is often depicted as triggers for accelerated economic strain, civil and social unrest, criminal activity and political insecurity.

Frequently portrayed as 'employment for stability', rigorous evidence on the issue of youth unemployment consistently demonstrates the nexus between youth unemployment and threats to peace and security. Although Azeng and Yogo's (2013) study predates more recent developments, their findings continue to hold scholarly value given its contemporary relevance. Examining the effects of youth unemployment on political instability among a sample covering 24 developing countries between 1980-2010, Azeng and Yogo's (2013) findings suggest that youth unemployment was significantly associated with an increase of risk of political instability, suggesting that the high rate of youth unemployment, compounded with socioeconomic inequalities and corruption, render countries more susceptible to political instability and national insecurity. These findings give credence to the warning issued by Teboho *et al.* (2024) that a lack of social and economic opportunities for youth increases the risk of uprisings, demonstrations and revolts, threatening state, national and human security.

The negative impact of youth unemployment on economic instability is well documented. Stagnant economic growth, poor investment and high unemployment is a consistent macroeconomic challenge for South Africa (Pasara *et al.* 2020). High unemployment negatively impacts economic growth (Makaringe *et al.* 2018); increases economic vulnerability (Monama *et al.* 2024); and minimises opportunities for further economic development (Sekwati *et al.* 2023. The study by Zungu *et al.* 2023) analysed the impact of income inequality and unemployment on crime in a panel of 15 African countries during the period 1994–2019. The authors conclude that economic development was found to decrease crime and make suggestions that, from a policy perspective,

policies targeting the distribution of income are crucial, as that might decrease income inequality and, at the same time, decrease crime. Against this backdrop, we see merit in the recent call issued in the 2024 Statistics South Africa Report (Statistics South Africa 2024) for addressing youth unemployment as a means to foster social cohesion, reduce inequality and importantly, as a vehicle to accelerate economic growth.

Crucial to national security is the extent to which people feel safe. There is much consensus that unemployment is the principal cause of many of the problems South Africa faces. The crime epidemic, not only in emerging economies but in many advanced economies too, continue to raise questions on the negative impact of unemployment. Prompted by this concern, Witte *et al.* (2019) established a robust connection between unemployment and crime in Europe. Their findings support their main hypothesis that a higher unemployment rate tends to increase non-violent crime thus suggesting that maintaining stable economic activity is critical to stabilize incidence of non-violent crime. In a 2015 study, Chitiga *et al.* (2015) investigated the effects of unemployment on the rate of crime in South Africa with specific reference to the Richards Bay and Empangeni communities in the KwaZulu-Natal Province. The investigation considered responses of 60 unemployed participants 20 experts on crime control and 30 convicts. The results indicate that low level of education is responsible for high unemployment rates which bears a direct relationship with the high rate of crime. Substantiating these findings in the South African context, Anderson *et al.* (2020) employed panel data from KwaZulu-Natal municipalities (2006-2017) and identified a positive and substantial association between youth unemployment and homicide rates, implicating labour market dysfunction as a contributory factor in provincial violent crime patterns. Similarly, a study examining the link between youth unemployment and violent crime, based on data from 2006 - 2016 for ten developing countries in Africa, including South Africa, found that youth unemployment and population growth increase violent crime (Adekoya 2020).

The nexus between high youth unemployment and crime, economic and political vulnerability, and social instability (Lebakeng & Notshulwana 2024; Monama & Mokoele 2024) cannot be disputed. As opined by Groenwwald 2023) South Arica's crime statistics reflect the level of criminality that is the direct consequence of a shrinking economy, and the desperation of unemployed South Africans who are increasingly resorting to crime for survival. With this in mind, we agree with the analysis of Lanzas (2022) that 'youth quiescence is merely a part of a much broader paralysis of a labour force confronted both by

rising unemployment and by a government which has been unwilling to grant to the leadership of labour any serious say in the business of the regulation of the economy' (p. 1). In the section below, we consider some of the strategies currently employed at addressing South Africa's youth unemployment crisis.

## Strategies Aimed at Reducing Youth Unemployment

The South African government has instituted a number of policies and frameworks aimed at addressing the problem of high youth unemployment. Most notably, South Africa's 2030 National Development Plan (NDP) issues optimism in its endeavours to, by 2030, 'create enough opportunities for all those who want to work to have the possibility of doing so' (p. 26). Building on the 2030 NDP, the National Youth Policy for 2020-2030 (NYP 2030) was subsequently formulated. The NYP 2030 is informed by various legislative frameworks including, for example, South Africa's Constitution, the National Development Plan (NDP 2030), National Youth Service Framework (2002), National Youth Development Agency (NYDA), African Youth Charter (2006), and well as the Sustainable Development Goals (SDGs). The NYP 2030 has implemented numerous strategies and interventions with the view to achieve 'an recommended, holistic and sustainable youth development, conscious of the diversities, historical imbalances and current realities, in building capacities for young people, so that they can in turn contribute their full potential in building a better life for all' (p. 7). Informed by the NYP 2030, is the establishment of the Youth Employment Service (YES). The YES works to provide employers across various sectors with resources and incentives to create 12-month quality jobs opportunities for youth. Other initiatives include, for example, the Expanded Public Works Programme (EPWP) which provides short term employment opportunities within the unskilled and semi-skilled sectors; the Youth in Agriculture and Rural Development Programme (YARD) which encourages engagement in agribusiness as well as the National Youth Service Programme (NYSP) which focuses on entry into various community service projects. In an endeavour to promote economic growth, foster self-sufficiency and encourage innovation the National Youth Development Agency (NYDA) and the Small Enterprise Development Agency (SEDA) make provisions for support and resources needed to cultivate a culture of entrepreneurship among youth.

While not fully addressing South Africa's youth unemployment pro-

blems, some successes have been noted. For example, Ndlovu and van der Merwe (2021) reflect on the YES programme initiative as successfully improving employment participation among youth. Other initiatives have noted some success too in improving youth employment rates including the EPWP programme (Chirwa & Mchombu 2022) and various entrepreneurship programmes (Nzama & Khumalo 2022). Unfortunately, despite these arguably limited successes, it is unfortunate that the NYP 2030 has failed to provide a concrete way out of the youth unemployment problem highlighting what Zwane (2020) considers be the outcome of an uncoordinated government which makes many good-intentioned proposals sound like pipe dreams. Phokontsi's (2021) analysis suggests that the impact of the various strategies employed by NYP 2030 are not reported in a manner that outlines their effectiveness and efficiency in dealing with youth development and employment. Similarly, further criticisms highlight that, despite 30 years into democracy, and various promissory endeavours, youth remain frustrated with a lack of economic opportunities and participation (SAIIA 2024). Notwithstanding various interventions made in policy and the labour market, youth continue to be at the core of the unemployment challenge. As Mtwesi (2014) points out, there are no shortages of structures, policies and plans for youth development however, the non-delivery on the part of government departments and youth institutions represents a lost opportunity and failure to comprehend the role youth play in society.

Persistent and critically high youth unemployment has validated the NDP 2030's cautionary forecast: unresolved employment challenges pose 'a serious threat to social, political and economic stability' (p. 16). In this context, we present potential pathways to deal with the South Africa's chronic youth unemployment problems.

## Future Directions

There is no shortage on opinions regarding the way forward. The idea of entrepreneurship as a panacea to the employment crisis is commonplace with frequent suggestions around advancing financial and infrastructural support and youth targeted entrepreneurship policy development (Ndlovu *et al.* 2024; Mammals 2022; Jubane 2021) to increases in economic involvement opportunities for youth. Bridging the skills-demand mismatch and promoting the development of 21st century skills through relevant education and training (SAIIA 2023) is frequently emphasised, with recommendations for accelerated efforts to expand vocational training opportunities (Mayombe 2021) developing

skills that are both technical and non-technical (soft skills) (Habiyaremye *et al.* 2022). Commonplace, too, is the urgent call for reforms to governance and economic policy (Akinola *et al.* 2023; Sibande *et al.* 2022) – often flagged as a pivotal solution to the youth unemployment crisis.

Upon careful analysis, what emerges as central to many the strategies considered worthwhile in fight against critically high youth unemployment, is a well-coordinated effort involving a range of stakeholders. Graham *et al.* (2018) emphasises that the means to achieving an inclusive society lies in a carefully coordinated system and commitment of various stakeholders. Echoing this perspective, Lannoy *et al.* (2020) call for a coordinated multi-stakeholder approach involving educators, trainers, employers, non-governmental organisations and government officials, arguing that such systemic coordination is essential to achieving meaningful reductions in youth unemployment.

Together, these strategies can translate the NYP 2030's vision into practice by coordinating interventions across quality education, skills development, labour market access and youth economic participation. A recurrent critique of South Africa's policy landscape is its implementation gap. Despite formulating policies that are often celebrated as progressive, robust and conceptually sound, the country struggles to convert policy intent into tangible outcomes. The NYP 2030's vision to enable youth to achieve their full potential across social, economic and political domains hinges critically on effective policy implementation. Without bridging the gap between policy and institutional practice, these aspirations will remain unrealized.

## Conclusion

The nexus between South Africa's youth unemployment crisis and risks to the nation's peace and security is evident. We reaffirm our position that South Africa's prosperity is hinged on its ability to resolve youth unemployment. Failure to address this crisis will perpetuate seemingly intractable problems of economic strain, civil and social unrest, criminal activity and political instability. As history dictates, robust policy alone will not be sufficient. The youth unemployment crisis demands carefully considered, well-coordinated efforts that translate the nation's sound legislative frameworks, policies and commitments into practice; prioritizing education, improving economic performance, and advancing the NDP 2030 vision of creating sufficient opportunities for all who seek employment.

## References

Adekoya, A.F. 2020. Youth Unemployment and Violent Crime: Evidence from Developing Countries in Africa. Universitatea SPIRU HARET - Faculty of Accounting and Financial Management. Available at: https://www.spiruharet.ro

Azeng, T.F. & T.U. Yogo 2013. Youth Unemployment and Political Instability in Selected Developing Countries. (Working Paper No. 171.) African Development Bank. Available at: https://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/Working_Paper_171__Youth_Unemployment_and_Political_Instability_in_Selected_Developing_Countries.pdf

Akwu, N. 2023. Youth Unemployment in South Africa can be Reduced: Pragmatic Policy Possibilities. Available at: https://ddp.org.za/blog/2023/06/07/youth-unemployment-in-south-africa-can-be-reduced-pragmatic-policy-possibilities/

Anderson, S. & M. Wilson 2020. Unemployment, Social Instability, and the Rise of Political Violence in Developing Countries. *International Journal of Economic Policy in Emerging Economies* 8,3: 205 - 218. https://doi.org/10.1080/23322039.2020.1799480

Baah-Boateng, W. 2016. The Youth Unemployment Challenge in Africa: What are the Drivers? *The Economic and Labour Relations Review* 27,4: 413 - 431. https://doi.org/10.1177/1035304616645030

Bhana, A. 2024. Unemployment Drops to 32.1% in Third Quarter. *Mail & Guardian.* Available at: https://mg.co.za/business/2024-11-12-unemployment-drops-to-32-1-in-third-quarter/

Bhattacharya, R. & V. Kumar 2019. The Impact of India's Skill Development Programs on Youth Employment. *Indian Journal of Development Economics* 14,2: 104 - 119.

Chidzikwe, M., January 2024. Empower Africa's Youth to Create Jobs, Growth, and Peace. World Economic Forum. Available at: https://www.weforum.org/stories/2024/01/empower-africa-s-youth-to-create-jobs-growth-and-peace/

Chirwa, E. & K. Mchombu 2022. Assessing the Impact of the Expanded Public Works Programme (EPWP) on Youth Unemployment in South Africa. *Development Southern Africa* 39,3: 350 - 365.

Chitiga, M. & R. Chitiga, R. 2015. Crime and Unemployment in South Africa: Revisiting an Established Causality - Evidence from the Kwazulu-Natal

Province. ResearchGate. Available at: https://www.researchgate.net/publication/272708608_Crime_and_Unemployment_in_South_Africa_Revisiting_an_Established_Causality_Evidence_from_the_Kwazulu_Natal_Province

Costa, A.M. & L.P. Santos 2021. Evaluating Brazil's 'First Employment' Program: Successful Outcomes for Youth Integration. *Latin American Economic Review* 58,3: 134 - 148.

Cristina, L. 2022. Workless Youth as a 'Moral Panic'. https://doi.org/10.4324/9781003308591-3

De Lannoy, A., L. Graham, M. Patel & M. Leibbrandt 2018. What Drives Youth Unemployment and What Interventions Help: A Systematic Overview of the Evidence and a Theory of Change. High-level Overview Report.

Department of Women, Youth and Persons with Disabilities 2020. Draft National Youth Policy 2020 - 2030. Available at: https://www.gov.za/sites/default/files/gcis_document/202007/nypdraft-2030-28-july-2020.pdf

Dimakatso, S., M.A. Dagume 2023. Effect of Unemployment and Inflation on Economic Growth in South Africa. *International Journal of Economics and Financial Issues*. https://doi.org/10.32479/ijefi.13447

Gbenga, W., A. Akinola & A. Ohonba 2023. Youth Unemployment and the Rising Crime Rate in South Africa: Does Governance Matter? Preprints. https://doi.org/10.21203/rs.3.rs-3298339/v1

Groenwald, T., 30 August 2023. Crime Statistics Reflect Impact of Unemployment. Freedom Front Plus. Available at: https://www.vfplus.org.za/media-releases/crime-statistics-reflect-impact-of-unemployment/

Habiyaremye, A., T. Habanabakize & C. Nwosu 2024. Bridging the Labour Market Skills Gap to Tackle Youth Unemployment in South Africa.

Idris, I. 2016. Youth Unemployment and Violence: Rapid Literature Review. University of Birmingham. Applied Human Services. https://gsdrc.org/wp-content/uploads/2016/11/YouthUnemployment_Violence.pdf

International Labour Organization n.d. Global Unemployment Rate Set to Increase in 2024 while Growing Social Concerns Loom. International Labour Organization. Available at: https://www.ilo.org/resource/news/global-unemployment-rate-set-increase-2024-while-growing-social (Accessed on 11 December 2024.)

International Labour Organization 2024. Global Employment Trends 2024. Available at: https://www.ilo.org/sites/default/files/2024-08/GET_2024_EN.pdf

International Labour Organization 2024. World Employment and Social Outlook: Trends 2024. Available at: https://www.ilo.org/sites/default/files/2024-06/WESO_May2024%20-%20Final_30-05-24_2.pdf

International Labour Organization 2020. Promoting Decent Employment for African Youth: A Peacebuilding Strategy. International Labour Organization. Available at: https://www.ilo.org/publications/promoting-decent-employment-african-youth-peacebuilding-strategy

Ivanov, D. & A. Morozov 2020. Russia's Approach to Youth Unemployment: A Case Study of the 'Youth Labor Exchange' Program. *Russian Journal of Labor Economics* 25,1: 89 - 102.

Jubane, S.M. 2021. Strategies for Reducing Youth Unemployment in South Africa. World Conference on Child and Youth 1: 1 - 11. https://doi.org/10.17501/26731037.2020.2101

Maramura, T., T. Makaye & T. Mude 2024. Inequality, Unemployment, and Poverty in the COVID-19 Era in Eastern Cape Province, South Africa. In Chrysostome, J., K. Kiyala & N. Chivase (eds.): *Climate Change and Socio-political Violence in Sub-Saharan Africa in the Anthropocene: Perspectives from Peace Ecology and Sustainable Development*. Cham, Switzerland: Springer Nature. https://doi.org/10.1007/978-3-031-48375-2_12

Mafalda, F., A. Luís & M.R.C. António 2020. O caso dos jovens nem nem: novas trajetórias, novos desafios. *Praxis Education* 16,42: 7348. https://doi.org/10.22481/PRAXISEDU.V16I42.7348

Mtwesi, A. 2014. An Overview of Youth Policy. *The Journal of the Helen Suzman Foundation* 74. Available at: https://www.hsf.org.za

Meyer, D.F. & P. Mncayi 2021. An Analysis of Underemployment among Young Graduates: The Case of a Higher Education Institution in South Africa. *Economies* 9,4: 196. https://doi.org/10.3390/economies9040196

Mncayi, P. & D.F. Meyer 2022. Evaluating the Determinants of the Perceptions of Underemployment among Young University Graduates: A South African University Case. *Cogent Social Sciences* 8,1: 2054126. https://doi.org/10.1080/23311886.2022.2054126

Mngoma, N.F. & O.A. Ayonrinde 2023. Mental Distress and Substance Use among Rural Black South African Youth Who are Not in Employment,

Education, or Training (NEET.) *International Journal of Social Psychiatry* 69,3: 532 - 542. https://doi.org/10.1177/00207640221114252 PMid:35903872 PMCid:PMC10152210

Molobela, T.T. 2023. Graduate Unemployment in South Africa: A Critical Examination of Determinants and Government Interventions. *African Journal of Development Studies* 13,4: 107 - 127. https://doi.org/10.xxxx/ajds.xxx

Monama, S.A. & N.J. Mokoele 2024. Idle Time and its Repercussions on Youth in South Africa: A Recipe for the Unemployment Crisis. *Journal of Business and Social Review in Emerging Economies* 10,2: 203. https://www.publishing.globalcsrc.org/jbsee

Moyo, M. & T. Mncube 2023. Youth Employment and Skills Development in South Africa: An Evaluation of the Skills Development Act. *Journal of Vocational Education and Training* 75,2: 214 - 229.

Munyati, C., 22 January 2024. Empower Africa's Youth to Create Jobs, Growth, and Peace. *World Economic Forum.* Available at: https://www.weforum.org/stories/2024/01/empower-africa-s-youth-to-create-jobs-growth-and-peace/

Ndlovu, T. & P. van der Merwe 2020. South Africa's Youth Employment Service (YES) Program: Achievements and Lessons Learned. *South African Journal of Economic Development* 38,2: 87 - 101.

Nzama, T. & S. Khumalo 2022. The Role of Entrepreneurship Programs in Addressing Youth Unemployment in South Africa. *Journal of African Business* 23,4: 456 - 470.

Pasara, M.T. & S.H. Dunga 2022. Unpacking South Africa's Structural Unemployment: A Critical Analysis. *AfricaGrowth Agenda* 19,1: 4 - 8.

Pasara, M.T. & R. Garidzirai 2020. Causality Effects among Gross Capital Formation, Unemployment, and Economic Growth in South Africa. *Economies* 8,2: 26. https://doi.org/10.3390/economies8020026

Phokontsi, G.L. 2021. A Governance Perspective on Policies and Practices Combating Youth Unemployment in South Africa. Doctoral dissertation, University of the Free State. https://scholar.ufs.ac.za/items/e736f775-67b4-42fd-9daa-0fec17825c53

Sakiel, A., N. Monama & J. Mokoele 2024. Idle Time and its Repercussions on Youth in South Africa: A Recipe for the Unemployment Crisis. *Journal of Business and Social Review in Emerging Economies* 10,2. https://doi.org/10.26710/jbsee.v10i2.2730

Solutions for Youth Employment (S4YE) n.d. Youth Employment Service (YES.) Available at: https://www.s4ye.org/node/4196

South African Institute of International Affairs 2024. South Africa: Realising Youth Futures by Delivering on Promised Goals. https://saiia.org.za/research/south-africa-realising-youth-futures-by-delivering-on-promised-goals/ (Accessed on 13 December 2024.)

Smith, J., 11 November 2023. Job Search Struggles and Unemployment in South Africa. *The New York Times.* https://www.nytimes.com/2023/11/11/world/africa/job-search-unemployment-south-africa.html

Snyder, H. 2019. Literature Review as a Research Methodology: An Overview and Guidelines. *Journal of Business Research* 104: 333 - 339. https://doi.org/10.1016/j.jbusres.2019.07.039

Statistics South Africa (StatsSA) 2024. Quarterly Labour Force Survey (QLFS) Quarter 1: 2024. Available at: https://www.statssa.gov.za/publications/P0211/P02111stQuarter2024.pdf

Statistics South Africa (StatsSA) 2024. Quarterly Labour Force Survey (QLFS) Q2: 2024. Available at: https://www.statssa.gov.za/publications/P0211/Presentation%20QLFS%20Q2%202024.pdf

Statistics South Africa (StatsSA) 2024. Quarterly Labour Force Survey (QLFS) Quarter 3: 2024. Available at: https://www.statssa.gov.za/publications/P0211/P02113rdQuarter2024.pdf

Teboho, J., K. Lebakeng & M. Notshulwana 2024. Demographic Youth Bulge and Unemployment as Potential for Political Violence and Insecurity in Africa, with Special Reference to South Africa. *Commonwealth Youth and Development.* https://doi.org/10.25159/2663-6549/13931

Webster, J. & R.T. Watson 2002. Analyzing the Past to Prepare for the Future: Writing a Literature Review. *Management Information Systems Quarterly* 26,1: 3.

Zwane, N., 24 March 2020. Draft National Youth Policy 2030 Offers a Glimpse into how Uncoordinated State Machinery is. *Daily Maverick.* https://www.dailymaverick.co.za/opinionista/2020-03-24-draft-national-youth-policy-2030-offers-a-glimpse-into-how-uncoordinated-state-machinery-is/

Dr. Shanya Reuben
Psychology
School of Social Sciences
University of KwaZulu-Natala
Durban
reuben@ukzn.ac.za

Ms. Shaida Bobat
Psychology
School of Social Sciences
University of KwaZulu-Natal
Durban
bobats@ukzn.ac.za

# Chapter 13: Social Dialogue as a Vehicle to Address Peace and Security – An Analysis of the BRICS Formal Declarations

**Nirmala Devi Gopal**
**ORCID iD: https://orcid.org/0000-0002-5104-0083**

**Cresencia Nyathi**
**ORCID iD: https://orcid.org/0009-0002-1355-4224**

## Abstract

The international community has witnessed a plethora of conflict, violence, and violent extremism, all leading threats to international peace and security. This paper examines how the BRICS (Brazil, Russia, India, China, and South Africa) have tackled global peace and security through formal declarations[1] using a social dialogue approach. Throughout 2013 to 2022, the analysis indicates a transition from a focus on economic matters to encompassing broader social and political concerns in these ten declarations. In this study, thematic analysis was employed to investigate the content of the BRICS formal declarations. The findings suggest that the summits have expanded their focus from purely economic matters to encompassing social and political issues. The study highlights the importance of a democratic UN Security Council, peaceful conflict resolution, cybersecurity, and international cooperation. It suggests the BRICS approach to peace and security should be enhanced through multilateral cooperation, gender integration, cybersecurity collaboration, conflict resolution, inclusive social dialogue, and global governance reforms.

**Keywords:** BRICS, peace and security, declarations, summits, social dialogue

[1] Durban, Fortaleza, Ufa, Goa, Xiamen, Johannesburg, Brasilia, Moscow, New Delhi and Beijing.

## Introduction

Global security is a key focus for the BRICS countries as they navigate the evolving landscape of globalisation. Peace and security are critical for global stability, prosperity, and the well-being of individuals, communities, and nations (Hassan, Fausat & Funmilola 2016). Thus, global security seeks to address the diverse and complex threats to international peace and stability, such as political instability, military conflicts, weapons proliferation, terrorism, cyber-attacks, and environmental degradation, among others (Abdenur 2016). In addressing global security issues, several international instruments have been formulated, which include the United Nations Charter, the UN Convention on the Law of the Sea, the Vienna Convention on Diplomatic Relations, the Geneva Conventions, the Hague Conventions, the North Atlantic Treaty Organisation (NATO), the Organisation for Security and Co-operation in Europe (OSCE), the Non-Proliferation Treaty (NPT), the Comprehensive Nuclear-Test-Ban Treaty (CTBT), and the Biological and Toxin Weapons Convention (BTWC). The UN Charter outlines the purposes and principles of the United Nations, including maintaining international peace and security (Trahan 2022). The charter empowers the Security Council to take collective action to address threats to international peace, including authorising the use of military force, imposing economic sanctions, and establishing peacekeeping operations (Blank 2023).

The 2008 global financial crisis triggered non-Western countries (Naik 2018) like China, Brazil, and India to have discussions about the 'crisis, global governance, and the liberal world order' (Lagutina 2019: 442). During the same period, the international community experienced a plethora of conflict, violence, organised, crime, and violent extremism (Sixpence, Makoni & Moyo 2021), leading to threats to international peace and security. Conflicts in Central Africa, Sahel, Ukraine, Syria, and Yemen have led to thousands of deaths and displacements (Nkiese & Wirba 2023). State fragility and weak institutions have facilitated the growth of hybrid organisations, posing global security and financial risks (Ficek 2022). These threats to peace and security have shaped the BRICS declarations with a specific focus on how peace and security might be enhanced.

Against this backdrop, the social dialogue approach (negotiation, information sharing, consultation, joint decision-making and joint problem-solving) emerged as a mechanism for addressing global peace and security threats using the BRICS formal declarations. The study explored how BRICS

summits from 2013 to 2022 utilised multilateral social dialogues to address peace and security issues. By emphasizing social dialogue, the research highlights its potential to mitigate conflict and foster integration, peace, and international unity. This study significantly contributes to international relations and peace and security literature by offering insights into the role of emerging economies in global governance and peacebuilding efforts. It builds upon existing research, such as Khambule, Biyela and Mthuli (2019); Abb and Jetschke (2019), by highlighting how BRICS nations influence global politics through cooperative dialogue and strategic diplomacy.

The need for novel approaches to peace and security is highlighted by the study's motivating factors, which include the escalation of international tensions, the shortcomings of current international institutions, and the demand for a more inclusive and representative global governance structure. With their focus on global social discussion and cooperation, the BRICS nations present a viable path towards tackling these issues. The study addresses pressing global concerns, provides policymakers with useful implications, and aids in the creation of fresh frameworks for resolving conflicts. To address global economic and social inequality and promote global peace and security, it underscores the necessity of restructuring international institutions to be more representative.

Through an examination of the BRICS nations and their formal declarations from eThekwini in 2013 to Beijing in 2022, the research seeks to reveal the potential of social dialogue as a means of resolving conflicts and promoting peace. This is especially pertinent in a world where established power institutions are under threat and non-Western voices are playing a bigger role in determining global governance (Brosig 2019a). With their varied histories and substantial worldwide sway, the BRICS nations provide a special viewpoint on matters of peace and security (Hooijmaaijers 2021). Through an examination of their official statements, the research aimed to comprehend how these nations work together to tackle these issues and what part social discourse plays in their approaches. This has applications for international organisations, scholars, and decision-makers.

The study examines how BRICS declarations from 2013-2022 attempt to address peace and security through the lens of the social dialogue approach. With the abovementioned issues, the paper focuses on the ten formal declarations from eThekwini in 2013 to Beijing in 2022 because of the expansion of engagement in various areas and BRICS's desire to communicate a more comprehensive and unified stance on key issues affecting the

international community. The paper starts by tracing the formation of the BRICS, followed by reviewing the literature on BRICS and its role in addressing global peace and security threats, as well as social dialogue. The paper then shows how the BRICS countries, through their formal declarations, attempt to address peace and security through the lens of the social dialogue approach. The paper contributes to BRICS' role in peace and security, by proposing that global security threats can be addressed through multilateral social dialogue.

## Tracing the Formation of BRICS

Since BRICS's inception as a multilateral organisation and its inaugural summit in 2009, it has highlighted a 'strong commitment to multilateral diplomacy with the UN playing the central role in dealing with global challenges and threats' (BRIC 2009) and assisting the international community with bringing about international peace and security. These commitments have been evident in their joint declarations from the eThekwini Declaration of 2013 to the Beijing Declaration in 2022.

In examining the BRICS formal declarations, the way the member states attempt to address peace and security threats needs to be grasped from a multilateral social dialogue framework. In 2012, we note that the BRICS announced itself as a platform for dialogue and cooperation that represents the needs of emerging and developing nations (BRICS 2012). This is based on the fact that the socio-economic and political policies that BRICS pursue to transform are within the 'international system which is riddled with imbalances in global governance and uneven development' (Khambule, Biyela & Mthuli 2019: 131). To achieve this, the BRICS use coexistence to achieve their goal of a global order free of hegemons.

## Global Peaceand Security Threats

The BRICS declarations consistently address peace and security issues by highlighting the importance of maintaining global stability through peaceful resolutions and multilateral cooperation (Brosig 2019a). For instance, the 2013 Durban Declaration calls for the peaceful resolution of conflicts, specifically mention-ing Syria, and supports multilateralism and adherence to international law (Abdenur 2016). The 2014 Fortaleza Declaration emphasizes UN peacekeeping missions and the peaceful settlement of disputes. In the 2015 Ufa

Declaration, BRICS nations committed themselves to joint efforts in combating terrorism and extremism, highlighting the need for international cooperation in cybersecurity. The 2016 Goa Declaration addresses global security threats, including terrorism, and advocates for UN Security Council reforms to include more representation from developing countries, reflecting a broader commitment to global peace and security.

The 2017 Xiamen Declaration stresses collaboration in public health to improve pandemic preparation in addition to highlighting cooperative efforts to combat terrorism and extremism (Khambule, Biyela & Mthuli 2019). The commitment to multilateralism and peaceful dispute resolution is reaffirmed in the Johannesburg Declaration of 2018. The BRICS nations tackle global security issues such as cyber threats and terrorism in the 2019 Brasília Declaration. The 2020 Moscow Declaration highlights the value of peaceful conflict resolution and multilateralism, especially in light of the COVID-19 pandemic (Petrone 2023) The 2021 New Delhi Declaration reiterates support for multilateralism while bolstering counterterrorism cooperation. The 2023 Johannesburg Declaration highlights peaceful conflict resolution and support for multilateralism as critical measures, whereas the 2022 Beijing Declaration concentrates on current global security concerns, such as regional conflicts and terrorism.

To bolster these commitments, the BRICS organised joint military exercises to enhance regional security and increase cooperation in peacekeeping operations (Abiola *et al.* 2017; Brosig 2019a). For instance, the BRICS joint military exercise in 2017 took place in India, while Exercise Indra-2017 was a collaborative effort between India and Russia. Additionally, the Russia-India-China (RIC) trilateral format included joint military drills, and the BRICS peacekeeping exercise was held in South Africa in 2018 (Brosig 2019a). Also, BRICS nations have consistently supported UN peacekeeping missions, including providing troops and financial resources to these missions (Abiola *et al.* 2017). Examples include India's participation in missions in Congo and South Sudan (Choedon 2023), China's involvement in Mali and the Democratic Republic of Congo (Cabestan 2018), Brazil's leadership in Haiti (Beauvoir 2022), South Africa's contributions in Sudan (Alchin, Gouws & Heinecken 2018), and Russia's support in Cyprus and the Middle East (Delanoe 2013).

Cyberspace is an essential component of modern society in a world infused with technology and information. However, digital organised crime (Di Nicola 2022) is making the international environment more and more volatile. International security is at risk because of many users' cyber risks and threats. With this threat, the activities and actions of the BRICS nations in cybersecurity

have remarkably increased in importance over the past few years (Belli 2021a) as cybercrimes have critical global implications, both politically and economically (Kshetri 2015). In 2017, BRICS nations signed a BRICS Joint Declaration on Cybersecurity Cooperation (Belli 2021b) to address emerging threats and promote a peaceful, secure, and open cyberspace.

Furthermore, the 2013 BRICS Summit in Durban, South Africa, acknowledged the need for international cooperation in cybersecurity. In recognition of the significance of 'contributing to and participating in a peaceful, safe, and open cyberspace', the 2013 eThekwini Declaration advocated for the development of 'universally acknowledged norms, standards, and practices' (BRICS 2013). Since 2013, the BRICS nations have developed and implemented a wide range of policies, rules, and legislation targeted at developing and testing their cybersecurity ideas. The BRICS leaders established the Working Group on Security in the use of ICTs in response to the 2015 Ufa Declaration with the goal of 'developing practical cooperation with each other to address common security challenges in the use of ICTs' while 'sharing information and case studies on ICT policies and programs'. This latter reason is fundamental because it explains why the objectives of the BRICS nations' policy challenges and solutions are becoming more and more similar.

The need to tackle cybercrime has seen BRICS countries domesticating and formulating legislation. For example, Brazil updated its cybersecurity strategy, passed a new data protection law, and proposed legislation to control social media content known as the 'Fake News Bill' in 2020 (Kshetri & DeFranco 2020). Russia approved its Internet Sovereignty Law, which intends to defend the nation against cyberattacks and, if necessary, permits disconnecting the Russian Internet from the more extensive Internet (Litvinenko 2021). India also proposed the new Personal Data Protection (PDP) Bill and made headlines (Gupta & Naithani 2022) for its new Information Technology Intermediary Guidelines and Digital Media Ethics Code Rules, 2021 (IT Rules). The Chinese National People's Congress passed the new Personal Information Protection Law (PIPL) in August 2021, which established new legal rights to privacy and the protection of personal information (Huang 2021). South Africa also witnessed significant changes to its digital policy by passing the South African Protection of Personal Information Act and updating the South African Cybercrimes Act in June 2021 (Snail ka Mtuze 2022), bringing the nation up to speed with global best practices.

The BRICS nations have also played a role in countering terrorism through various means, such as joint statements and declarations condemning

terrorism. BRICS has demonstrated a firm and united position against terrorism, denouncing it in every form. Their statements emphasize that no act of terrorism can be justified, and the member nations are committed to enhancing their collaboration to prevent and combat international terrorism. This joint effort is vital for maintaining global security and safeguarding human lives.

BRICS countries have collectively opposed the use of unilateral sanctions, which they believe undermine global peace and stability (Kapustin & Khabriev 2019). The BRICS countries condemn unilateral sanctions, arguing they undermine international law and UN authority, cause economic hardship, and are often imposed without considering potential consequences. They advocate for a coordinated approach through the UN and multilateral institutions (Thakur 2014). BRICS leaders, including Brazil, resisted unilateral sanctions at the 11th BRICS Summit in 2019, advocating for a coordinated, collective approach to global security and economic issues and expressing their opposition to sanctions in international forums like the United Nations General Assembly and the World Trade Organisation (WTO). Instead, they advocate for a more coordinated and collective approach to address international security and economic issues, through the UN and other multilateral institutions (Stuenkel 2015). These declarations demonstrate the BRICS countries' commitment to promoting a more cooperative and multilateral approach to international relations and their belief that sanctions should only be imposed by international law and with the approval of the United Nations.

The BRICS countries have expressed their opposition to military interventions and have called for peaceful resolution of conflicts through diplomatic means. In 2015, the BRICS declared in the Ufa Declaration that there is no military solution to the conflict in Ukraine and that reconciliation requires inclusive political dialogue. In 2015, the BRICS declared in the Ufa Declaration (2015) that there is no military solution to the conflict in Ukraine and that reconciliation requires inclusive political dialogue. From the above, the Declaration confirms the commitment of the BRICS to resolving conflicts non-violently. They believe that military interventions can exacerbate conflicts, result in the loss of innocent lives, and undermine the principles of international law and the authority of the United Nations (Zifcak 2015).

At the 2017 BRICS Summit, leaders underlined conflict resolution through political and diplomatic means and condemned force violations in violation of the United Nations Charter (Odeyemi 2016). BRICS countries have shown support for peaceful dispute resolution and regional stability and security through institutions like the United Nations and the Shanghai Cooperation

Organisation (Kirton & Larionova 2022). The BRICS countries are committed to promoting peace and stability in the international community, believing in conflict resolution through diplomatic, peaceful means, international law, and United Nations Charter principles.

In addition, BRICS countries have called for reforms of the United Nations Security Council (UNSC) to make it more representative, democratic, and effective in addressing global security challenges (Petrone 2021). BRICS advocates for the UNSC's reform to include more developing countries, particularly from Africa and Latin America, to ensure their perspectives are represented and decisions are made through a more democratic and inclusive process (Weiss & Abdenur 2014). The BRICS leaders at the 9th BRICS Summit in 2017 called for an early reform of the UNSC, promoting a more democratic and representative global governance system, reflecting changing power dynamics and the growing importance of developing countries.

In 2013, the eThekwini Declaration welcomed the World Conference on Human Rights (Lobato 2018). It showed commitment to exploring cooperation as global challenges also contributed to human rights violations of different groups of society. The BRICS members, through the summits, have managed to project a unified vision to denounce human rights violations and called for a human rights approach to resolving conflicts. The Ufa Declaration commits to promoting constructive human rights dialogue at international forums, including the United Nations, promoting a multifaceted social dialogue approach for conflict resolution.

## Social Dialogue for Peace and Security in BRICS Countries

The BRICS countries utilise social dialogue to address global issues threatening peace and security, distinguishing it from its common use as an engagement. The International Labour Organisation (ILO) defines social dialogue 'as a participatory development approach that includes all types of negotiation, consultation, or simply an exchange of information between, or among, representatives of governments, employers, and workers on issues of common interest relating to economic and social policy' (Ishikawa 2003: 3). From the definetion, one can deduce that social dialogue encourages the role of different groups of society at various levels to participate in socioeconomic and policy issues. The social dialogue process can be informal, institutionalised, or both. Khambule (2014: 41) concurs with ILO (2003) that 'social dialogue is a mechanism of participatory partnerships, joint problem-solving, and decision-making'.

BRICS countries are utilising social dialogue as a strategy to tackle globalisation challenges, acknowledging the crucial role of all parties in conflict in promoting peace and security (Kirton & Larionova 2022). The utilisation of social dialogue has unearthed the understanding that ongoing political and socio-economic threats require collective efforts to mitigate their effects effectively. Social dialogue techniques (negotiation, information exchange, consultation, collaborative decision-making, and joint problem-solving) have arisen as strategies for increasing collective response to global developmental challenges in response to this context (Khambule, Biyela & Mthuli 2019).

The guiding principle of the social dialogue approach is the belief that social partners can only meaningfully contribute when allowed to participate in peace and security issues. With this ideology, the BRICS countries have risen to create a global community motivated by shared developmental goals (De Coning, Mandrup & Odgaard 2015). The effectiveness of BRICS countries' social dialogue in addressing global peace and security challenges depends on their implementation and the willingness of other international actors to engage in dialogue and cooperation.

Furthermore, BRICS nations are implementing social dialogue principles, focusing on peaceful dispute resolution and cybersecurity challenges, and enhancing cooperation and trust. The Anti-Terrorism Working Group guides these strategies and offers lessons for global entities (Ndzendze 2020). Social dialogue among BRICS countries has fostered trust and cooperation, addressed conflicts, and found common ground (Jordaan 2021). They have also adopted a holistic approach to peace and security, focusing on human rights, root causes, and long-term, sustainable peace through systematic and structural reforms to eliminate violent relations (Khambule, Biyela & Mthuli 2019). Therefore, the use of social dialogue by BRICS for conflict resolution aligns with constructive theories such as collaborative learning theory and communicative action theory (Er, Dimitriadis & Gašević 2021), stressing dialogue, negotiation, and collaboration (Ajonbadi, Mordi & Adekoya 2023).

Social dialogue promotes inclusivity, prevents conflicts, builds trust, and promotes democratic governance (Ishikawa 2003; Khambule 2014; Ajonbadi, Mordi & Adekoya 2023). It involves diverse stakeholders, including marginalised groups, in decision-making, ensuring transparency and legitimacy. In addition, social dialogue is an inclusive approach that considers diverse perspectives, promoting transparency and legitimacy. It addresses societal tensions, promotes ownership, and maintains peaceful societies (Khambule, Biyela & Mthuli 2019). However, effective implementation requires time, re-

sources, and commitment from all parties involved. However, despite its benefits, it can be slow, time-consuming, and challenging to coordinate diverse stakeholders, potentially marginalising weaker ones and leading to deadlocks (Galgóczi 2020). Policies developed through social dialogue are more effective and sustainable (Carré & Steiert 2022). These enable the parties involved to take ownership and accountability in the implementation of the policies. However, social dialogue often fails to achieve peace and security due to its weak implementation and insufficient follow-up mechanisms post-agreement (Khambule 2014). It tends to focus narrowly on specific issues, overlooking broader systemic problems like economic inequality or political exclusion. External interference from geopolitical dynamics can distort outcomes, aligning them with external interests rather than local needs (Steen & Nauta 2020). Institutional weaknesses, including lack of capacity and authority, undermine the enforcement of agreements. Thus, the exclusion of key stakeholders, such as armed factions, limits the dialogue's effectiveness in addressing underlying causes of conflict.

From 2013-2022, BRICS declarations prioritised peace and security, with the 2013 Durban Declaration establishing global governance, promoting peace and initiating dialogues on reforming international institutions. The 2014 Fortaleza Declaration underlined international peace and cooperation in combating terrorism. BRICS nations have called for the finalisation of the Comprehensive Convention on International Terrorism (Ndzendze 2020) and have underscored the need for international cooperation in counter-terrorism efforts. This led to the establishment of the BRICS New Development Bank (Cooper 2017) for infrastructure and sustainable development thereby indirectly contributing to stability within member nations. The 2015 Ufa Declaration and 2016 Goa Declaration highlighted peaceful conflict resolution through dialogue and diplomatic solutions, stressing intelligence sharing and collaborative counter-terrorism efforts in regions like Syria and Ukraine. The Xiamen Declaration in 2017 and the Johannesburg Declaration in 2018 stressed the link between global economic governance and peace, promoting inclusive growth and multilateral cooperation.

The 2019 Brasília Declaration and 2020 Moscow Declaration underscored the importance of sustainable development and long-term peace, while the COVID-19 pandemic stressed global health and security coordination (Di Nicola 2022). The New Delhi Declaration in 2021 underlined post-pandemic recovery, security, and cooperation, leading to the 2022 Beijing Declaration advocating for high-quality partnerships and multilateralism to

tackle global challenges (Ficek 2022). BRICS member states have implemented principles outlined in declarations, including India's active participation in counter-terrorism initiatives, China's increased UN peacekeeping involvement, South Africa's mediating role in conflicts across Africa including Lesotho between 2014 and 2018 (Deleglise 2023), Brazil's improved cybersecurity capabilities, and Russia's focus on counter-terrorism and cybersecurity.

The BRICS declarations, including the Johannesburg II Declaration (2018), have not addressed xenophobia in South Africa, but other frameworks like the National Action Plan aim to. The declarations have faced implementation challenges due to varying national interests and priorities (Chaturvedi & Saha 2017) and a lack of robust mechanisms for monitoring progress (Vyas-Doorgapersad 2021). Social dialogues have been limited, and engagement with stakeholders has been insufficient (Öniş & Gençer 2018) for a more inclusive approach.

## Method

A qualitative research methodology guided the study. The case study of the BRICS countries uses a theoretical framework of social dialogues to examine how formal declarations address peace and security challenges. We have adopted a qualitative research process to understand how the group addresses global threats in their everyday words. Qualitative data was drawn from journal articles, policy papers, reports, and press statements. The BRICS formal declarations from 2013 to 2022 provide the basis for this study's data set. A thematic analysis approach based on coding was used to investigate the meanings of the formal declarations generated on the BRICS, which reveal the priority areas of the BRICS. The themes are not found in the declarations but are 'derived' and 'actively crafted' by the researcher, reflecting their interpretative choices, instead of pre-existing analysis' (Braun, Clarke & Weate 2016: 740). Fugard and Potts (2015: 669) posit that thematic analysis 'is not about counting words or phrases, but a qualitative method for uncovering a collection of themes'. In this context, it is used to unravel how the BRICS formal declarations on peace and security are organised through patterns to create meanings.

In explaining how the BRICS have harnessed social dialogues inaddressing peace and security, only issues speaking about peace and security were selected, and the recurrence of some themes over the years was identified. The first phase started with familiarising ourselves with the clauses that speak

to peace and security. The second step consisted of formulating abstract categorical proposals to connect the open codes and finding relationships among them. The third step involved identifying an umbrella or central theme to capture the essence of the other sub-categories.

We used Rivas's approach for coding themes and analysing data. It begins with identifying code titles in the data and continuing the process until 'gaps in the data are filled or new and unexpected themes unpacked' (Rivas 2012: 369). The end of the process is reached 'when no new themes emerge from the data (which is called saturation of themes)' (Rivas 2012: 369). Similar to Rivas's (2012) zig-zag approach, when identifying the themes or code titles in the initial stages of analysing the BRICS annual summit declaration statements, we started in chronological order with the 2013 declaration up until the 2022 declaration. The following themes emerged from the analysis of the formal declarations: reforms of the UNSC and the inclusivity of the developing countries, resolution of global conflicts, internal conflicts and low profile on security issues.

## Thematising the BRICS Formal Declarations on Peace and Security

### *Theme 1: Reforms of the UNSC and Inclusivity of the Developing Countries*

The group also raises important positions at the international platforms. They have been vocal since the 2013 to 2022 summits in demanding reforms in the traditionally established international financial institutions such as the United Nations Security Council (UNSC), the International Monetary Fund (IMF), the World Trade Organisation (WTO), and the World Bank (WB). During the summit in Brazil in November 2019, the BRICS called for an 'urgent need' to strengthen and reform the UN and other multilateral organisations, including the World Trade Organisation (WTO) and the IMF, to address the significant challenges being faced by developing countries (BRICS 2019).

The results show that there is a recurring need for more poor nations to be represented in international organisations, with reforms being called for in statements such as the 2013 Durban Declaration. However, as the 2015 Ufa Declaration points out, resistance from existing forces limits development. The 2013 Durban Declaration and other declarations show that the BRICS have continuously pushed for increased representation of poor nations in inter-

national organisations (Lobato 2018). As stated in the 2015 Ufa Declaration, established powers' resistance, however, limits genuine development. One can recommend the creation of strategic relationships and solid plans to improve these initiatives. The call for reformation is influenced by the fact that the SC is still outdated because it still reflects the post-World War era. Most importantly, Africa needs representation in the group of permanent members (Abb & Jetscke 2019). This reveals that the BRICS have used their cooperation as a platform to advocate for the inclusion of developing countries in the critical structures of the UNSC. The formal declarations strategically convey inclusive participation and a call for equity as one of the commitments of the BRICS states.

## *Theme 2: Resolution of Global Conflicts*

The BRICS countries are concerned with ongoing conflicts across the globe. This is expressed in their declarations as they denounce most ongoing conflicts in regions like North Africa, the Middle East, and West Africa (Lagutina 2019). Their interest in these conflicts occurring in other nations stems from the negative repercussions these conflicts have on those nations. For instance, regarding security, Russia is highly concerned about the Middle East's Arab Spring-related rise in terrorism and Islamic fundamentalism spreading to the Caucasus region (Dannreuther 2015). Russia has increased security measures in the North Caucasus to combat radical ideologies and prevent terrorism, while its intervention in Syria aims to stabilise the region and reduce extremist influence. Additionally, concerns about domestic unrest and the impact of Middle Eastern instability on global oil prices have prompted Russia to position itself as a counterbalance to Western influence in the region. Additionally, Russia was worried about stabilising Afghanistan due to a rise in opium production in the nation that has been imported into Russia and was posing a threat to national security due to an increase in heroin addiction (Mohammed 2015).

Particular cyberattacks, like 2017's WannaCry (affected the United Kingdom, Russia, United States of America, China, Brazil and France) and NotPetya (affected Ukraine, Russia, USA, Germany, France, Poland and Italy), led the BRICS countries to prioritise international cybersecurity collaboration (Champagne *et al.* 2019). The necessity for global standards and procedures in cyberspace security was emphasized in the BRICS Joint Declaration on Cybersecurity Cooperation (Wanglai 2018). Terrorist acts such as the Paris attacks of November 2015 and the BRICS statements of Xiamen (2017) and Ufa (2015) denounced terrorism and promoted global collaboration in counter-

terrorism endeavours. These instances show how BRICS leverages official declarations to address issues related to international security by utilising cooperative social dialogues.

BRICS have made diplomatic statements which included statements on global peace and security issues, advocating for peaceful resolutions to conflicts (De Coning, Mandrup & Odgaard 2015). They have condemned acts of terrorism and called for international cooperation against terrorism (Wanglai 2018; Sixpence, Makoni & Moyo 2021). In general, the BRICS nations back the UN and other multilateral institutions as dispute resolution frameworks. In settling disputes, they place a strong emphasis on the value of international law and respect for national sovereignty. Through diplomatic channels, the BRICS countries have supported regional peace initiatives, even if they are not directly involved in mediating crises. For instance, they support regional organisations' efforts at mediation or promote peace accords. By promoting economic development and cooperation among member countries and with other nations, BRICS indirectly contributes to stability and conflict prevention. Economic development can reduce the underlying causes of conflict. BRICS encourages cultural exchanges and people-to-people contacts (Hooijmaaijers 2021), which can foster understanding and reduce tensions between nations.

## *Theme 3: Internal Conflicts*

The BRICS states that we share the vision of working together to address challenges threatening peace and security. Nevertheless, their collaboration 'hides the reality of a lack of unifying values, principles, goals and even interests among the group members' (Thakur 2014: 1792). The arguments stem from the fact that BRICS are different countries with separate contexts, histories, political and economic systems, needs, opportunities, and futures. Despite their domestic priorities and problems, they prioritise group solidarity. We examined how BRICS handles conflicts, which was imperative in understanding how they use formal declarations to address peace and security threats. The formal declarations reveal that BRICS can 'assume a business-as-usual or an institutional adjustment scenario' (Papa & Verma 2021: 539). This indicates that the group still needs to rethink how to exert collective leadership better to address contemporary peace and security challenges in global governance.

There are various global conflicts that BRICS members call for their peaceful resolution; however, they also, from time to time, have internal conflicts that need to be tabled during the summits. Internal conflicts can

threaten group solidarity, global peace, and security if resolved poorly. For example, China and India have underlying tensions over unresolved territorial claims, leading to confrontations in 2017 (Niu & Hong 2021). The group did not issue a joint statement about the conflict between China and India. Other members have attempted to downplay this conflict, and China and India would have considered it intrusive. As Brosig (2021) and Panova (2021) explain in this Special Section, BRICS' core principles (e.g., respect for sovereignty) and its operational mechanisms, such as the formal consensus rule and informal commitment not to import conflicts, suggest that BRICS do not fully address their internal conflicts. Vazquez's contribution notes that Brazil does not practice policy interventions in such disputes. Brosig (2021) highlights that South Africa will not officially interfere, although it formerly suggested that the group strengthen its peacebuilding cooperation. Panova (2021) argues that Russia thinks India and China can deal with the crisis themselves but will keep engaging them through the Russia-India-China group, the Shanghai Cooperation Organisation, and other bodies as needed. In other words, this conflict is formally a non-issue for BRICS.

Compartmentalisation is a strategy where different areas of cooperation are kept separate, and conflicts in one area do not affect cooperation in other areas (Papa & Verma 2021). The BRICS has adopted this strategy to manage internal conflicts and differences among the member countries. For example, even though the BRICS countries may have differences on certain issues, such as sanctions, military interventions, or human rights, they have continued to cooperate and coordinate their actions in other areas, such as economic development, regional stability, and global governance reform. Within the BRICS, disagreements may also arise due to economic concerns. For instance, China's Belt and Road Initiative (BRI) has boosted Chinese influence and investment in areas where other members of the BRICS, such as Brazil and India, are also looking to grow their economic presence (Medeiros & Benvenuto 2020). Their combined approach to global economic governance and development activities may occasionally become less cohesive because of this competition. By adopting a compartmentalisation strategy, the BRICS countries have been able to maintain a strong commitment to cooperation and coordination, while managing their internal differences and conflicts.

Formally, BRICS does not have a conflict management mechanism for intragroup conflict resolution. Conflict management in international institutions is increasingly professionalised, and many institutions have functioning dispute settlement mechanisms. During the 2019 BRICS Legal Forum, BRICS recog-

nised the urgent need to establish BRICS Dispute Resolution Centres within BRICS member states. Still, the group focused on commercial rather than interstate disputes (Papa & Verma 2021). This was the progressive approach to setting up conflict resolution mechanisms to help address internal conflicts among the member states. The stances of individual BRICS members on international peace and security may also be influenced by the strategic alliances they have with non-BRICS nations. Some BRICS members, especially China and Russia, who have more antagonistic relations with Western powers, may have opinions that are not entirely aligned with those of the other members due to factors such as Brazil's relations with Western nations or India's strategic cooperation with the United States (Lieber 2014).

With Russia as one of the critical nations supporting the Syrian regime, the ongoing crisis in Syria is also causing concern among the BRICS nations. This advocacy runs counter to the BRICS' call for a dialogue process that is 'Syrian-led, Syrian-owned' as the only viable option. Given the economic ties between the Middle East, India, and China, a negotiated resolution with Russia may result (Jordaan 2021: 460). South Africa and Brazil, however, oppose taking military action in Syria. Furthermore, given the present Venezuelan situation, the BRICS members are only sometimes in agreement on resolving the dispute. Brazil is presently supporting the United States of America-backed opposition leader Juan Guaidó, partly distancing itself from the other BRICS members, while Russia, China, and South Africa are supporting Venezuelan President Nicolas Maduro and opposing US action (Panova 2021). India remains silent about the situation and maintains an essentially neutral position. Until recently, India has imported oil despite US sanctions against Venezuela, temporarily appeasing the US.

The goal of the BRICS alliance is to advance global multipolarity and modernise international governance systems. However, it might be challenging for them to present a unified front on global peace and security due to internal conflicts brought on by geopolitical rivalries, economic rivalries, and differing opinions on human rights and governance. Geopolitically, Russia's actions in Eastern Europe and unsolved territorial tensions like those between China and India strain relations (Singh 2023). Relationship hostilities may arise from past or present territorial conflicts or geopolitical rivalries among some BRICS members. For example, unresolved border disputes between China and India have resulted in military standoffs and tensions (Westcott 2022). Similarly, several BRICS nations have taken diplomatic positions in opposition to Russian actions in Eastern Europe, particularly its annexation of Crimea (Sjøli 2023).

Economic rivalry for influence, as seen by China's Belt and Road Initiative, makes group approaches to global governance more difficult (Medeiros & Benvenuto 2020). Furthermore, cohesion is made more difficult by differing perspectives on human rights and governance, which are made worse by strategic alliances with non-BRICS countries (Duggan *et al.* 2022). Notwithstanding these obstacles, the BRICS nations work together to address global concerns, provided that internal contention is controlled to successfully promote a more just international system.

## *Theme 4: Low Profile on Security Issues*

There are concerns about the BRICS members when it comes to security issues. The group tends to maintain a low profile on security issues. Never will BRICS try to turn the organisation into a conventional security system. For instance, the BRICS nations largely refrained from denouncing Russia's 2014 annexation of Crimea (Brosig 2019b). When Russia took Crimea in 2014, the group offered little to no criticism. They did not participate in a UN General Assembly vote that denounced Russia's takeover of Crimea. The BRICS nations opposed proposals to ban Russia from the G-20, significantly lessening the impact of Western efforts to isolate President Putin (Stuenkel 2014).

Numerous concerns have been voiced concerning the BRICS nations' adherence to the values of respect for territorial integrity and sovereignty, considering the current crisis between Russia and Ukraine. Considering current territorial and geopolitical challenges, reviewing these fundamental tenets that guide BRICS cooperation is essential. Voting at the United Nations General Assembly (UNGA) and UNSC strongly suggests that the BRICS vote 'together' solely on issues of common concern, such as multiple draft resolutions on Syria and general opposition to solutions that call for the use of force or sanctions. A thorough examination of the past voting trends for the BRICS at the UNGA on nuclear weapons demonstrates that member votes vary greatly. Brazil and South Africa both lack atomic weapons, and a key component of their foreign policies is the prevention of nuclear proliferation.

Brazil voted against the other members' abstention in the first vote to demand a stop to Russia's aggression against Ukraine. China and Brazil voted in favour of the resolution on March 24 to allow humanitarian access to the area, but India and South Africa boycotted due to the resolution's polarising nature. Another meaningful event was the vote to kick Russia out of the UN Human Rights Council. As the investigations into the Bucha massacre (reported abuse

and killing of Ukrainians by the Russian Armed Forces) continued, China voted against expelling Russia, and the other BRICS members stayed silent. China criticised the 'blind charges' against Russia at the time. This demonstrates the BRICS' primary goal, which is to expose Western insincerity and double standards to create an equal global order. Before the 2022 BRICS Summit, the foreign ministers of the BRICS nations released a joint statement in which they underscored their support for talks between Russia and Ukraine and their common worries about the ongoing humanitarian catastrophe.

## Multilateral Social Dialogues: Strengthening Peace and Security through Social Dialogue

The BRICS, through interregional interactions (Naik 2018), consistently calls for conflict transformation, which according to Lederach (2015), underlines peace as embedded in justice, the building of right relationships and social structures through radical respect for human rights, and nonviolence as a way of life. The BRICS Summit Beijing Declaration of 2014 indicates the commitment to resolve disputes peacefully. For example, Point of the Declaration elaborates, 'We commit to respecting the sovereignty and territorial integrity of all States, stress our commitment to the peaceful resolution of differences and disputes between countries through dialogue and consultation, support all efforts conducive to the peaceful settlement of crises'. The call for coexistence by the BRICS member states reveals that the international community acknowledges that social conflict is ordinary in human relationships and can be a vehicle for change (Lederach 2015).

Thakur (2014: 1797) elaborates that the BRICS states reject the militarisation of disputes and conflicts in the internal affairs of the independent states and are opposed to violations of territorial integrity and sovereignty. Such opposition can be driven by historical memories of invasion by the European powers, hence their fear of Western interference in their internal affairs. Furthermore, the 2013 to 2022 Declarations call for the international community to journey together to build healthy relationships and communities locally, regionally, and globally. More importantly, the member states continually hold meetings, for instance, National Security Advisers and High Representatives on National Security, as one of the ways to map resolutions to global threats. Most crucially, the conclusion of the 12th Meeting of the High Representatives for National Security and National Security Advisers of the BRICS, held on June 15, 2022, indicated the necessity of changing the modern

and current way diverse nations and communities relate to one another.

With existing big powers imbalances, competition, and the shift of the world order, the BRICS, through their Declarations, has utilised interregional social dialogues to address peace and security. All the ten Declarations under study have joint statements of commitment towards peaceful means. The Brasilia Declaration, Ufa Declaration, and Goa Declaration condemned terrorism, especially in the Middle East and North and West Africa. The other Declarations also are concerned with rampant terrorism which groups have executed like Al-Shabaab, Boko Haram, Al-Qaeda, Taliban, ISIS, and other affiliated groups. Such ongoing threats of terrorism reveal the need for conflicting parties to find common ground and map nonviolent ways for resolving conflicts. Succinctly, the BRICS states are encouraging the international community to adopt a helpful lens that brings varying aspects of conflict complexity into focus.

The BRICS also calls for the address of the root causes of the conflicts. For instance, the Fortaleza Declaration of 2014 Point 26 states the following:

> We recall that development and security are closely interlinked, mutually reinforcing, and key to sustainable peace. We reiterate our view that establishing sustainable peace requires a comprehensive, concerted, and determined approach based on mutual trust, mutual benefit, equity, and cooperation, that addresses the root causes of conflicts, including their political, economic, and social dimensions. In this context, we also stress the close interrelation between peacekeeping and peacebuilding. We also highlight the importance of bringing gender perspectives to conflict prevention and resolution, peacebuilding, peacekeeping, rehabilitation, and reconstruction efforts.

The abovementioned call shows the commitment of the BRICS to working with the international community to envision a framework that will address peace and security threats and create a platform to manage the context, content, and structure of the relationships between various states. Using social media, the conflicting parties can begin to find creative responses and solutions that promote peace and security. Importantly, it is high time that the international community plans long-term and deep systematic and structural peacebuilding reforms to eliminate the conditions that create and reproduce violent relations at international interaction levels. There is a need to shift the way the international community understands interregional interactions fundamentally.

The BRICS have harnessed the social dialogue approach, which is fundamental in achieving peace and security. Rather than looking at isolated conflict episodes, they have called for political dialogues (Fortaleza and eThekwini Declaration). Through this call, they have encouraged various parties to seek to understand how these episodes are embedded in the more significant pattern of human relationships and interregional coexistence. The call is for conflicting parties to move conflict away from destructive processes and toward constructive ones. This is fundamental to development, international security, and sustainable peace. They are not calling for quick solutions to immediate problems but rather to generate platforms that simultaneously address surface issues and change underlying social structures and relationship patterns.

The cooperation of the international community is a good recipe for addressing peace and security issues in BRICS countries. Briefly, social dialogue has the potential to improve interregional interactions as peace is centred and rooted in the quality of relationships. There is a possibility of peace when they are both face-to-face interactions and shared values. Hence, the member states continue to commit to working together towards that as peace and security are continuously evolving and developing the quality of relationships. With social dialogue as a participatory approach of various society stakeholders, the Declarations from 2014 are broadening and highlighting the 'importance of bringing gender perspectives to conflict prevention and resolutions, peacebuilding, peacekeeping, rehabilitation and reconstruction efforts' (Fortaleza Declaration 2014). More efforts are needed to address the natural rise of human conflict through nonviolent approaches that address issues and increase understanding, quality, and respect in relationships. More importantly, the BRICS states have acknowledged that the globe is confronted by political instability and conflicts in their Declarations and have called for action to resolve conflict amicably.

The BRICS concerns about violence and military interventions suggest that the international community needs to develop capacities to engage in change processes at the interpersonal, inter-group, and social-structural levels. Military interventions will not fully resolve the global challenges, hence the need to have the capacity to understand and sustain social dialogue as a fundamental means of constructive change. Indeed, many skill-based mechanisms that reduce violence are rooted in communicative abilities to exchange ideas, find standard definitions, and move toward solutions. But dialogue also plays a crucial role in maintaining or changing social structures. These structures can be modified through dialogue to be more responsive and just.

The BRICS countries have continued to build trust and cooperation amongst themselves using social dialogue that has promoted open communication and encouraged the sharing of ideas and perspectives (Khambule, Biyela & Mthuli 2019). By engaging in social dialogue, the BRICS countries have addressed conflicts and differences and found common ground on issues of mutual concern. Importantly, this approach has helped to enhance the legitimacy and effectiveness of the BRICS grouping by ensuring that the perspectives and interests of all stakeholders are considered and that the policies and practices of the BRICS countries are representatives of the global community. Therefore, social dialogue is a critical component of the BRICS countries' cooperation and coordination and is essential for addressing peace and security challenges.

## Conclusion

The BRICS summit from 2013 to 2022 utilised multilateral social dialogues to address peace and security issues. The study analysed the BRICS formal declarations, identifying key themes related to peace and security, and evaluating the effectiveness of the social dialogue approach. The study confirmed that social dialogue is a significant tool for BRICS countries in promoting global peace and security, demonstrating the need for continued international cooperation and the positive role of BRICS in global governance. However, the effectiveness of these declarations depends on the implementation of proposed solutions and the willingness of other international actors to engage in dialogue and cooperation.

## Recommendations

Recommendations for enhancing the BRICS approach include:

(i) strengthening multilateral cooperation;

(ii) integrating gender perspectives and human rights;

(iii) expanding cybersecurity collaboration, addressing conflict root causes;

(iv) promoting inclusive social dialogue mechanisms; and

(v) advocating for global governance reforms.

We argue that future research can explore implementation impacts, membership dynamics, and challenges in BRICS' peace and security agenda.

## References

Abb, P. & A. Jetschke 2019. The Devil is in the Detail: The Positions of the BRICS Countries towards UN Security Council Reform and the Responsibility to Protect. The Positions of the BRICS Countries towards UN Security Council Reform and the Responsibility to Protect. In Matthew, S.D. & M. Zürn (eds.): *Contested World Orders: Rising Powers, Non-governmental Organizations, and the Politics of Authority beyond the Nation-state*. New York: Oxford University Press. https://doi.org/10.1093/oso/9780198843047.003.0005

Abdenur, A.E. 2016. Rising Powers and International Security: The BRICS and the Syrian Conflict. *Rising Powers Quarterly* 1,1: 109 - 133.

Abiola, S., C. De Coning, E. Hamann & C. Prakash 2017. The Large Contributors and UN Peacekeeping Doctrine. In *UN Peacekeeping Doctrine in a New Era*. London: Routledge. https://doi.org/10.4324/9781315396941-7

Ajonbadi, H.A., C. Mordi & O.D. Adekoya 2023. The Realities of Social Dialogue and Trade Unions in Morocco. In Mordi, C., H.A. Ajonbadi & O.D. Adekoya (eds.): *Employee Relations and Trade Unions in Africa: A Critical Approach*. Cham, Switzerland: Palgrave Macmillan. Available at: https://link.springer.com/chapter/10.1007/978-3-031-26825-0_8 (Accessed 27 June 2023). https://doi.org/10.1007/978-3-031-26825-0_8

Alchin, A., A. Gouws & L. Heinecken 2018. Making a Difference in Peacekeeping Operations: Voices of South African Women Peacekeepers. *African Security Review* 27,1: 1 - 19. https://doi.org/10.1080/10246029.2017.1406381

Beauvoir, J.M. 2022. In Post-conflict Haiti, Brazil Consolidates its Status as Regional Actor. *STIMSON* Article ID(6).

Belli, L. 2021a. CyberBRICS: A Multidimensional Approach to Cybersecurity for the BRICS. In Belli, L. (ed.): *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*. Brazil: Springer. https://doi.org/10.1007/978-3-030-56405-6_1 PMCid:PMC8107835

Belli, L. 2021b. CyberBRICS: A Multidimensional Approach to Cybersecurity for the BRICS. *CyberBRICS: Cybersecurity Regulations in the BRICS*

*Countries* Article ID: 1 - 33. https://doi.org/10.1007/978-3-030-56405-6_1 PMCid:PMC8107835

Blank, L. 2023. Collective Security and the United Nations. In *International Conflict and Security Law*. UK: Edward Elgar Publishing. https://doi.org/10.4337/9781800377240.00007

Braun, V., V. Clarke & P Weate 2016. Using Thematic Analysis in Sport and Exercise Research. In *Routledge Handbook of Qualitative Research in Sport and Exercise*. New York: Routledge. https://doi.org/10.4324/9781315762012-26

BRICS 2009. *First Summit: Joint Statement of the BRIC Countries' Leaders*. Toronto: University of Toronto. Available at: www.brics.utoronto.ca/docs/index.html#goa (Accessed on 12 January 2023.)

BRICS 2013. *eThekwini Declaration and Action Plan*. Available at: http://brics5.co.za/aboutbrics/summit-declaration/fifth-summit (Accessed on 12 January 2023.)

Brosig, M. 2019a. Ten Years of BRICS: Global Order, Security and Peacekeeping. *International Peacekeeping* 26, 5: 521 - 526. https://doi.org/10.1080/13533312.2019.1677283

Brosig, M. 2019b. Ukraine: Moving Borders Changing Orders? In *The Role of BRICS in Large-Scale Armed Conflict*. Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-030-18537-4_5

Brosig, M. 2021. Has BRICS Lost its Appeal? The Foreign Policy Value Added of the Group. *International Politics* Article ID: 1 - 19. https://doi.org/10.1057/s41311-021-00327-y PMid:40479143 PMCid:PMC8253684

Cabestan, J.P. 2018. China's Involvement in Africa's Security: The Case of China's Participation in the UN Mission to Stabilize Mali. *The China Quarterly* 235: 713 - 734. https://doi.org/10.1017/S0305741018000929

Champagne, A., N. Drainville, C. Felt, Z. Gao, C. Herriford, E. Hobbs, M. Jain, N., N. Kalderash, S. Koeck & E. Krabill 2019. *International Cybersecurity: De-escalating Tensions in a Digital Era*. Washington: University of Washington. Available at: https://digital.lib.washington.edu/researchworks/bitstream/handle/1773/43755/TaskForce_B_Beyer.pdf?sequence=1 (Accessed 30 June 2024).

Chaturvedi, S. & S. Saha 2017. Competing Imperatives of Global Governance and National Interests within BRICS: An Indian Perspective. *Rising Powers Quarterly* 2,3: 167 - 183.

Choedon, Y. 2023. India's Development and Peacebuilding Assistance to the Conflict-affected States: Case-study of Democratic Republic of Congo. *International Studies* 60,1: 45 - 66. https://doi.org/10.1177/00208817231151609

Cooper, A.F. 2017. The BRICS' New Development Bank: Shifting from Material Leverage to Innovative Capacity. *Global Policy* 8,3: 275 - 284. https://doi.org/10.1111/1758-5899.12458

Dannreuther, R. 2015. Russia and the Arab Spring: Supporting the Counter-Revolution. *Journal of European Integration* 37,1: 77 - 94. https://doi.org/10.1080/07036337.2014.975990

De Coning, C., T. Mandrup & L. Odgaard 2015. Coexistence in between World Order and National Interest. In de Coning, C., T. Mandrup & L. Odgaard (ed.): *The BRICS and Coexistence. An Alternative Vision of World Order.* (Global Institutions.) Article ID: 171 - 181. https://doi.org/10.4324/9781315766171 PMid:24376165

Delanoe, I. 2013. Cyprus, a Russian Foothold in the Changing Eastern Mediterranean. *Middle East Review of International Affairs* 17,2: 84 - 93.

Deleglise, D. 2023. Conflict Mediation in Southern Africa and the Evolution of Institutionalised Mediation Support. *Mediating Peace in Africa: A Study on the Role of Mediation Support Units*. Article ID: 39. ACCORD.

Di Nicola, A. 2022. Towards Digital Organized Crime and Digital Sociology of Organized Crime. *Trends in Organized Crime*. Article ID: 1-20. Available at: https://link.springer.com/article/10.1007/s12117-022-09457-y (Accessed on 30 October 2022.) PMid:35669219 PMCid:PMC9148938

Duggan, N., B. Hooijmaaijers, M. Rewizorski & E. Arapova 2022. Introduction: The BRICS, Global Governance, and Challenges for South - South Cooperation in a Post-Western World. *International Political Science Review* 43, 4: 469 - 480. https://doi.org/10.1177/01925121211052211

Er, E., Y. Dimitriadis & D. Gašević 2021. A Collaborative Learning Approach to Dialogic Peer Feedback: A Theoretical Framework. *Assessment & Evaluation in Higher Education* 46, 4: 586 - 600. https://doi.org/10.1080/02602938.2020.1786497

Ficek, R. 2022. The Fragile States as a Challenge to the Contemporary International Security. *Rocznik Bezpieczeństwa Międzynarodowego* 16,1: 23 - 53.

Fugard, A.J.B. & H.W.W. Potts 2015. Supporting Thinking on Sample Sizes for Thematic Analyses: A Quantitative Tool. *International Journal of Social Research Methodology* 18,6: 669 - 684. https://doi.org/10.1080/13645579.2015.1005453

Galgóczi, B. 2020. Just Transition on the Ground: Challenges and Opportunities for Social Dialogue. *European Journal of Industrial Relations* 26, 4: 367-382. Available at: https://journals.sagepub.com/doi/abs/10.1177/0959680120951704 (Accessed 27 June 2024). https://doi.org/10.1177/0959680120951704

Gupta, I. & P. Naithani 2022. An Assessment of the JPC Report on PDP Bill, 2019. *Economic and Political Weekly* 57,31.

Hassan, B.D., A. Fausat & B Funmilola 2016. The Imperative of Peace and Security for the Attainment of Inclusive Growth in Nigeria. *European Journal of Research in Social Sciences* 4,2.

Hooijmaaijers, B. 2021. China, the BRICS, and the Limitations of Reshaping Global Economic Governance. *The Pacific Review* 34,1: 29 - 55. https://doi.org/10.1080/09512748.2019.1649298

Huang, J.J. 2021. Regulating Cross-border Information Flow – The Proposed Chinese Personal Information Protection Law. SocArXiv/ Ej5cx_v1. https://doi.org/10.31235/osf.io/ej5cx

Ishikawa, J. 2003. *Key Features of National Social Dialogue: A Social Dialogue Resource Book*. Geneva: International Labour Office.

Jordaan, A.C. 2021. BRICS – *Quo Vadis*? *Development Southern Africa* 38,3: 454 - 468. https://doi.org/10.1080/0376835X.2020.1870932

Kapustin, A. & B. Khabriev 2019. Unilateral Sanctions – A Vestige of a Unipolar World: The Conceptualization of the Legal Position of the BRICS Countries. *BRICS Law Journal* 6,4: 6 – 94. https://doi.org/10.21684/2412-2343-2019-6-4-67-94

Khambule, I. 2014. Institutionalising Social Dialogue. *Skills at Work: Theory and Practice Journal* 7,1: 41 - 52.

Khambule, I., A. Biyela & S. Mthuli 2019. BRICS, Coexistence and Social Dialogue : Towards a Multilateral Social Dialogue? *African Renaissance*, 16,2: 121 - 142. Available at: https://doi.org/10.31920/2516-5305/2019/V16n2a6 (Accessed 11 January 2023).

Kirton, J. & M. Larionova 2022. The First Fifteen Years of the BRICS.

*International Organisations Research Journal* 17, 2: 7 - 30. https://doi.org/10.17323/1996-7845-2022-02-01

Kshetri, N. 2015. Cybercrime and Cybersecurity Issues in the BRICS Economies. *Journal of Global Information Technology Management* 18, 4: 245 - 249. https://doi.org/10.1080/1097198X.2015.1108093

Kshetri, N. & J.F. DeFranco 2020. The Economics of Cyberattacks on Brazil. *Computer* 53,9: 85 - 90. https://doi.org/10.1109/MC.2020.2997322

Lagutina, M.L. 2019. BRICS in a World of Regions. *Third World Thematics: A TWQ Journal* 4, 6: 442 - 458. Available at: https://doi.org/10.1080/23802014.2019.1643781 (Accessed on 03 January 2023.) https://doi.org/10.1080/23802014.2019.1643781

Lederach, J. 2015. *Little Book of Conflict Transformation: Clear Articulation of the Guiding Principles by a Pioneer in the Field*. University of Colorado: Simon and Schuster.

Lieber, R.J. 2014. The Rise of the BRICS and American Primacy. *International Politics* 51: 137 - 154. https://doi.org/10.1057/ip.2014.1

Litvinenko, A. 2021. Re-defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty. *Media and Communication* 9,4: 5 - 15. https://doi.org/10.17645/mac.v9i4.4292

Lobato, L.V.C. 2018. The Social Issue in the BRICS Project. *Ciência & saúde coletiva* 23: 2133 - 2146. https://doi.org/10.1590/1413-81232018237.09072018 PMid:30020370

Medeiros, S.E. & L.M. Benvenuto 2020. The Chinese Belt and Road Initiative and Possible Repercussions to BRICS and Brazil: Facing Complexity under Uncertainty. *Journal of China and International Relations*. Article ID: 1 - 22. Available at: https://journals.aau.dk/index.php/jcir/article/view/4235 (Accessed on 30 June 2024.)

Mohammed, Y. 2015. The Middle East amid Global Multipolarity: The Emergence of New Actors in the Region Involving the BRICS Countries. *Revista InterAção* 8,8. https://doi.org/10.5902/2357797516837

Naik, S. 2018. Rising BRICS: A Path to Multipolar World Reality? *Сравнительная политика* 9,1: 100 - 108.

Ndzendze, B. 2020. BRICS and the Economics of Terrorism. *Latin American Report* 36,1: 1 - 23. https://doi.org/10.25159/2663-6581/8332

Niu, H. & S. Hong 2021. A Chinese Perspective: Will China - India Friction Paralyze the BRICS? *Global Policy* 12,4: 524 - 528. https://doi.org/10.1111/1758-5899.12968

Nkiese, J.K. & S.K. Wirba 2023. Perspective Chapter: Armed Conflict and Its Impact on Human Migration – The Healthcare Perspective. In Michaud, A., S.P. Stawicki & R. Izurieta (eds.): *Global Health Security - Contemporary Considerations and Developments*. IntechOpen.

Odeyemi, C. 2016. R2P Intervention, BRICS Countries, and the No-fly Zone Measure in Libya. *Cogent Social Sciences* 2,1: 1250330. https://doi.org/10.1080/23311886.2016.1250330

Öniş, Z. & A.S. Gençer 2018. Democratic BRICS as Role Models in a Shifting Global Order: Inherent Dilemmas and the Challenges Ahead. *Third World Quarterly* 39,9: 1791 - 1811. https://doi.org/10.1080/01436597.2018.1438185

Panova, V.V. 2021. Age of Multilateralism: Why is BRICS Important Despite Possible Weaknesses? A Perspective from Russia. *Global Policy* 12,4: 514 - 518. https://doi.org/10.1111/1758-5899.13013

Papa, M. & R. Verma 2021. Scenarios for BRICS Evolution in Light of the India - China Conflict. *Global Policy* 12,4: 539 - 544. https://doi.org/10.1111/1758-5899.13010

Petrone, F. 2021. BRICS and Global Governance: Will the Grouping be Able to Reform the United Nations Security Council? *International Studies* 58,3: 363 - 379. https://doi.org/10.1177/00208817211029409

Rivas, C. 2012. Coding and Analysing Qualitative Data. *Researching Society and Culture* 3: 367 - 392.

Singh, R. 2023. Russia, India, and China Alliance - Towards Balancing the World Order. *Indo - Asian Geopolitics: Contemporary Perspectives by DRaS.* Article ID: 111. Available at: http://www.ejsss.net.in/uploads/172/14313_pdf.pdf (Accessed on 30 June 2024.)

Sixpence, P., C. Makoni & C. Moyo 2021. Islamic Propagation and the Threat of Radicalisation and Violent Extremism (Rve) in Southern Africa. Examining the Vulnerabilities of Zimbabwe. *Indiana Journal of Humanities and Social Sciences* 2,3.

Sjøli, J.N. 2023. The BRICS: An Alliance for Peace? A Study of Discourses in Brazil, India, China and South Africa around the Russian War in Ukraine (2014 - 2023). Master in Political Science and Management, University of Agder.

Snail ka Mtuze, S. 2022. The Convergence of Legislation on Cybercrime and Data Protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013.

*Obiter* 43: 536 - 569. https://doi.org/10.17159/obiter.v43i3.14883

Social Europe without Social Dialogue: Decision of the Court of Justice of the European Union in C-928/19 P 2022. Article ID VS/2017/0434, 315 - 333. Cambridge University Press. Available at: https://doi.org/10.1017/S1574019622000177 (Accessed on 27 June 2024.)

Steen, M. & J. Nauta 2020. Advantages and Disadvantages of Societal Engagement: A Case Study in a Research and Technology Organization. *Journal of Responsible Innovation* 7,3: 598 - 619. Available at: https://www.tandfonline.com/doi/pdf/10.1080/23299460.2020.1813864 (Accessed 30 June 2024). https://doi.org/10.1080/23299460.2020.1813864

Stuenkel, O. 2014. Why Brazil has not Criticized Russia over Crimea. *Policy Brief, Norwegian Centre for Conflict Resolution - NOREF*, Article ID: 1 - 3.

Stuenkel, O. 2015. The G7 and BRICS in the Post-Crimea World Order. *Russia in Global Affairs* 13,2: 128 - 138.

Thakur, R. 2014. How Representative are BRICS? *Third World Quarterly* 35, 10: 1791 - 1808. https://doi.org/10.1080/01436597.2014.971594

Trahan, J. 2022. Vetoes and the UN Charter: The Obligation to Act in Accordance with the 'Purposes and Principles' of the United Nations. *Journal on the Use of Force and International Law* 9,2: 243 - 277. https://doi.org/10.1080/20531702.2022.2059882

Vyas-Doorgapersad, S. 2021. Global Governance Reforms to Achieve Sustainable Development Goal One (No Poverty) in BRICS. *Africa's Public Service Delivery & Performance Review* 9,1: 9.

Wanglai, G. 2018. BRICS Cybersecurity Cooperation: Achievements and Deepening Paths. *China International Studies* 68: 124.

Weiss, T.G. & A.E. Abdenur 2014. *Introduction: Emerging Powers and the UN – What Kind of Development Partnership?* Taylor & Francis. https://doi.org/10.1080/01436597.2014.971583

Westcott, S.P. 2022. Seizing a Window of Opportunity? The Causes and Consequences of the 2020 Sino-Indian Border Stand-off. *Journal of Asian Security and International Affairs* 8,1: 7 - 32. Available at: https://journals.sagepub.com/doi/pdf/10.1177/2347797021992527 (Accessed 27 June 2024). https://doi.org/10.1177/2347797021992527

Zifcak, S. 2015. What Happened to the International Community? R2P and the Conflicts in South Sudan and the Central African Republic. *Melbourne Journal of International Law* 16,1: 52 - 85.

Professor Nirmala Devi Gopal
Criminology and Security Studies
Department of Criminology & Forensic Studies
Howard College Campus
University of KwaZulu-Natal
Gopal@ukzn.ac.za

Dr. Cresencia Nyathi
Post-Doctoral Fellow
Department of Criminology and Forensic Studies
Howard College Campus
University of KwaZulu Natal
cresencia.nyathi@gmail.com

# Chapter 14: Institutional Investors in Russia: Security Problems and Prospects

**Irina Yarygina**
**ORCID iD: https://orcid.org/0000-0001-8684-1684**

**Vladimir Smirnov**
**https://orcid.org/0000-0002-1243-5349**

## Abstract

The objective reasons for assessing the role of institutional investors as secure and valuable participants of the Russian financial market and forecast trends within the framework of various projects is explained by the necessity of optimizing their participation in serving the needs of national and international economy as well as using the tools of environmental policy promotion. The subject of the research is the activity of institutional investors in contemporary environment and possible ways of making them as secure financial intermediaries more effective in providing the needs of the modern economy, especially in the fuel and energy complex as a key sector of the Russian Economy. The article provides a comparative analysis of the current set of factors and threats that affect the prospects of participation of institutional investors in financial markets. The complex analysis methodology, used in assessing the problems, involves considering the standpoint of the influence of a set of factors, subdivided into internal and external. Internal factors include the national market conditions and environmental issues. External factors reflect the long-term impact of a potentially adverse or favourable impact on the course of projects implementation, based on institutional investors' facility in spite of market turbulence or political sanctions.

**Keywords:** institutional investors, financial security, national economy, international cooperation, fuel and energy complex

Modern institutional investors are defined as special financial institutions that manage savings in the interests of private investors, maintain an acceptable level of risk, with the intent of obtaining the maximum investment return, backed by the terms and conditions of an agreement, which highlights their important role in ensuring the security of the national economy. Institutional investors (II) comprise collective investment institutions, pension funds, and insurance companies. II participate in the process of direct (on their name) and indirect financing (as agents) and perform the following economic functions:

- they are responsible for the efficient distribution of financial resources among economic entities;
- accumulate savings of the population and reduce transaction costs; and
- diversify risks and participate in the environment protection.

The term 'institutional investors' is interpreted in the Russian economic literature relatively broadly and includes both non-deposit and deposit intermediaries. Some authors limit themselves in listing most financial intermediaries as institutional investors. At the same time experts of the Bank for International settlements define insurance companies, pension funds and various collective investment schemes as institutional investors. In several studies of Russian economists the institutional investors are considered as non-bank financial intermediaries who invest funds, accumulated in course of their activity, in financial market instruments in order to gain profit.

We believe that retail banks cannot be classified as classic institutional investors, since their activity is related to attracting deposits and placing them in loans, while institutional investors are mostly focused on long-term investments.

It is worthwhile mentioning that the term 'collective investment' is also widely used in the Russian Federation and related to non-state pension funds and specialized companies. Sometimes, so-called collective investors are involved in raising funds from a large number of individuals for their subsequent investment as institutional investors.

Thus, to define prospects and problems of institutional investors as security actors, it is important to clear up the issue of identity of the institutional investor and the institution of collective investment.

## Methodology

The research used different methods: comparative analysis, content analysis and complex analysis. The method of comparative analysis is used to determine the influence of institutional investors on contemporary economy and identify the role of institutional investors as participants of financial markets. The content analysis method made it possible to assess the role of institutional investors as participants of the financial market and forecast trends of developments within the framework of implementing various projects. In general, the collected data allows us to understand the trends of economic and financial situation and form evaluative judgment about the problems and prospects for institutional investors activity in contemporary environment. The complex analysis method is used to systematize a set of factors and threats that affect the prospects of II participation in financial markets. The complex analysis methodology involves considering the object of assessment from the standpoint of the influence on it of a set of factors, subdivided into internal and external. Internal environment factors include the national market conditions. External factors reflect the long-term impact of a potentially adverse or favourable impact on the course of projects implementation based on institutional investor's facility in spite of market turbulence or political sanctions.

## Results and Discussions

International practice often uses the term 'asset management industry', that refers to the II activity. It is known that the subject of asset management can be property owners as well as professional managers. Moreover, the management object is private and clients funds. Thus, institutional investors as financial intermediaries, operate in the asset management industry and we can distinguish the following essential features of institutional investors as financial security actors:

- accumulation of funds of individual and corporate investors;
- accumulated resources management as a single portfolio; and
- long-term portfolio investments in securities;

Taking into consideration the mentioned features we come to conclusion, that insurance companies, pension funds (PF), and collective investment

institutions (collective investments), endowment funds can be defined as Institutional investors.

We define the trends of slowing down the process of globalization of financial markets and growing cyber activity of the market as well as participation of II in different projects.

Globalization was the key factor of the financial markets' development for a definite period. We confess the new stage of its development – economic partnership of globalized environment, manifested in integration of financial instruments, market participants, regulatory authorities, securities trading mechanisms, and unification of rules and regulations.

Having a wide range of investment options, institutional investors, do not limit themselves to financial assets available on domestic markets. The increasing efficiency of information technologies and the easing of regulatory restrictions have contributed to their global activity. The trend towards formation of a global investment environment and integration of national capital markets to the global context has accelerated investments in foreign assets and usually purchase securities, depository receipts, shares of investment funds, derivative financial instruments.

It is worthwhile mentioning that pension funds operate in the national and international markets and invest up to 30% of their assets in international instruments and markets. Thus, we come to conclusion, that contemporary stage of market development accelerates the cross-border supply of services by institutional investors and gives way to life insurers and pension funds to attract funds and contribute to the sustainable economic development on the national and supranational level, which fully corresponds to the current situation in Russia.

We consider that the main trend manifest itself in developing the resource base of green projects requests improvement of production and environment protection base. For example, the International Energy Agency (IEA) estimates that prevention of major climate changes by reducing carbon emission, additional $500 billion is required to be invested annually, in addition to the $10.5 trillion of investments in 2010-2030. At the same time BP experts consider, that in the nearest future approximately two thousand hydroelectric power plants will operate worldwide. It is important for strategic development and planning, which fully corresponds to the current situation in Russia.

Institutional investors have accumulated a significant amount of capital and the variety of instruments, well known to financial professionals that can help to smooth out the consequences of a significant slowdown in global

economic growth. Acceleration of II activity will be a positive trend that will contribute to sustainable development of the global economy.

Due to the flexibility and mobility (along with huge assets and other advantages), institutional investors play a significant role in the global financial architecture, that is confirmed by their cooperation with supranational structures, changes in the composition and direction of global capital flows and environmental policy measures which change the role of institutional investors in global economy, turning them into systemic financial institutions.

II play an important role in the global economy that should be considered in formation of Russia's short-term and long-term economic strategy. Analysis has proved that institutional investors control more than 80 percent of the US stock market capitalization. At the same time, private investors, implementing a policy of strategic investment of company assets, control only 10 percent of the UK market. The consequence of such kind of II participation in the market is a trend of their significant control over business and its financing. Thus, we consider it both positive and negative. On the one hand, institutional investors provide companies with broad access to financing, which plays a huge role in modern economy. On the other hand, there is a trend of market monopolization and formation of unofficial cartel agreements due to operational control of different players in the same segment of the market by one group of investors.

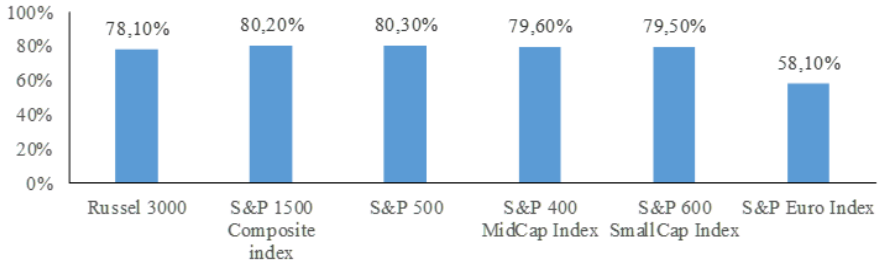



**Figure 1**. Institutional investors' ownership of the largest US stock indices.
**Source:** 80% of equity market cap held by institutions / / Pensions and Investment Magazine, 2023

It should also be noted that according to Bloomberg, different kind of institutions own more than 80 percent of the shares of the ten largest US companies.

Investment funds control assets totalling more than $ 18 trillion, which on average is about 24% of the GDP of the organization's member countries.

Pension funds and insurance companies control assets with a total value of 21.4 and 7 trillion US dollars 37% and 15% of GDP, respectively).

**Table1 - Investment funds assets in relation to GDP**

| **Volume of assets in relation to GDP** | **2009** | **2019** |
|---|---|---|
| Austria | 44% | 45% |
| Belgium | 24% | 38% |
| Canada | 43% | 103% |
| Chie | 0% | 0% |
| Czeck Republic | 3% | 8% |
| Danmark | 0% | 110% |
| Estoni | 3% | 4% |
| Finland | 23% | 54% |
| France | 69% | 73% |
| USA | 69% | 116% |
| Russia | 1% | 3% |

**Calculated based on OECD data // https://stats.oecd.org/**

Table 1 indicates the very little involvement of institutional investors in the economy of the Russian Federation. It seems appropriate to expand activity of pension funds, endowment funds and other specialized financial institutions - players in the financial market in order to use resources in solving strategic tasks.

As can be seen from the table above, in most countries the share of investment funds during 2009 - 2023 significantly increased in many countries. The share of their assets greatly exceeds the GDP of some countries. Thus, we can conclude that the financial sector prevails in the economies of these countriesб that requires attention to administration management.

Practice has demonstrated the experience that is of an interest. The most popular investment tools for institutional investors are shares and units of

various investment funds. It is important to note that in the period of 2009 - 2022, the volume of assets placed in the mentioned tools exceeded the share of debt instruments such as corporate bonds and Federal loan bonds. Another important trend is the refusal of investors to increase placement of their funds with banks (deposits), caused by the difference of the interest rates of the banks and global financial market.

**Table 2. Value of assets of institutional investors in million US dollars**

| Asset value | 2009 | 2022 |
|---|---|---|
| Deposits | 4 181 116 | 4 450 829 |
| Debt instruments | 22 329 853 | 23 234 58 |
| Loans | 3 378 084 | 3 375 834 |
| Shares and units of investment funds | 21 289 707 | 24 863143 |

**Calculated based on OECD data // https://stats.oecd.org/**

The most attractive areas of investments in the Russian Federation is the infrastructure development. The most popular type of projects are the following.

*Roads*. The volume of investments amounted to more than 10 billion US dollars. The main forms of participation were concession agreements and investments through market infrastructure funds.

*Airports*. The volume of investments is about 1 billion US dollars with participation through infrastructure funds.

*Gas transportation infrastructure* in the United States, Mexico, and Australia. The volume of investments amounted to more than 20 billion US dollars. The main form of participation is investment through market infrastructure funds.

*Investment in energy assets*. The total volume of this category is about 1.5 billion US dollars. Participation is carried out by using debt financing, direct investments, as well as participation in market infrastructure funds

We may distinguish the following classification of mutual funds in infrastructure financial market, depending on the structure (accumulation) of their assets, such as money market funds, bond funds, equity funds, mixed investment funds, private equity funds, high-risk (venture) investment funds, fund of funds, rental funds, estate funds, mortgage funds, index funds (with index indication), credit funds, foundations of the commodity markets, hedge funds, foundations of artistic values, environment protection funds.

The UN set benchmarks in 2015 for achieving the 2030 Sustainable Development Goals, stating that they must 'meet the requirements of the present without compromising the ability of future generations to meet their needs'. For this, it is important to reconcile three pillars: economic growth, social inclusion and environmental protection. These elements are interrelated and critical to the secure well-being of individuals and society'[1].

Deterioration of the environment directly affects the quality of life of the population. Therefore, consumers began to vote with money in favor of goods that are produced in accordance with the principles of sustainable development. A March 2020 poll by the Capgemini Research Institute found that 79% of consumers change their shopping habits to reflect the impact of their purchases on social or environmental issues (Jacobs *et al.* 2022).

This kind of demand is converted into indicators that are significant for companies. Standard & Poor's notes that from January 2010 to December 2022, the average monthly growth in the shares of companies with the lowest carbon dioxide emissions and accounting for 20% of the total number of companies in the MSCI World Index (developed markets) was 25 basis points higher than the 20% of companies in this Index with the worst such emission (Falk *et al.* 2023). Bank of America Merrill Lynch found that firms with better ESG performance than their peers were more likely to turn into high-quality stocks, less likely to have significant price declines, and less likely to go bankrupt (Subramanian 2022). In addition, socially responsible companies have the opportunity to raise

[1] The Sustainable Development Agenda. What is sustainable development? United Nations. URL: https://www.un.org/sustainabledevelopment/development-agenda (дата обращения (15 July 2020).

borrowed funds from banks at lower interest rates compared to companies with similar financial reliability that do not take ESG risks into account in their activities (Kordsachia 2023). The cost of capital for companies that adhere to ESG principles is about 10% lower than for other companies, since investors believe that they have lower risks in terms of non-compliance with environmental legislation (Bernow, Nuttal & Brown 2023).

The potential benefits of investing in projects implementing environmental protection programs are clear for the Russian authorities. Therefore, the analysis of possible risks associated with environmental pollution is very important, especially for large investment projects that provide for long payback periods and are typical for institutional investors, including portfolio investments of pension funds, national wealth funds, etc.

The topic of climate risks for portfolio and institutional investors, including sovereign funds, has become relevant only in the last 10-15 years. Moreover, in different parts of the world they are perceived differently. If earlier the main topic of the pre-project study was the financial analysis of the investment object, then in 2021 in Europe just over 50% of investments were made taking into account the factors of sustainable development, and in the USA the share of such investments in stocks was about 25% (Eccles 2019).

Currently, the only generally accepted quantitative objectively verifyable indicator of environmental risk is the price of a ton of carbon dioxide emitted by an enterprise. Wherein, investors take into account in the financial analysis the possible costs of greenhouse emissions, regardless of whether such costs are incurred at the national level or not, because the regulatory rules can change quickly.

As we can see, measures to improve the climate significantly affect the efficiency of investments. On the other hand, as the Boston Consulting Group and the Global Financial Markets Association in their fundamental research on climate finance in December 2021 noted that while the need for financing climate projects around the world is 100-150 trillion US dollars, the role of institutional investors is very important: in the equity investments they provide it accounts for 35% of the total funding requirement, and in bonds - 21%[2].

High economic and political risks associated with sanctions pressure, the Russian Federation is on the path of economic development through substitution of European and American sources of financing, as well as optimization

[2] Climate Finance Markets and the Real Economy. Boston Consulting Group and the Global Financial Market Association (December 2022: 178).

of domestic financial resources (Brayley & Myers 2023). An important role in this regard is played by institutional investors who can participate effectively in the implementation of development programs.

According to our calculations, the public and private sectors invested about 5.7 trillion rubles (2022) in infrastructure development, which is 200 billion rubles (3.6%) more than a year earlier. However, insurance companies and pension funds have no experience of participating in big projects, as a result, their share in capital investments is insignificant.

Investments in infrastructure remain attractive for private funds, but their money is getting into the industry too slowly. We consider that the main reason is the lack of projects structured under bonds.

At the end of 2022, the share of corporate bonds in the investment portfolio of national private funds (NPF) decreased by 6 percentage points, to 45% (1.2 trillion rubles), while the share of Federal loan bonds (OFZ) increased sharply to 28% (0.7 trillion rubles), from 10% in the first half of the year. In monetary terms, NPF investments in Russian OFZs more than tripled, from 235 billion rubles to 739 billion rubles. Thus we can conclude, that the activity of private investment funds should be supported by public authorities, if the invest in social or industrial sector.

VEB (Vnesheconombank of the Russian Federation) since 2003 has been a state management company for the trust management of pension savings and since 2012 VEB performs the functions of a state management company for the funds of the payment reserve. VEB's activity is carried out in accordance with the legislation of the Russian Federation, regulatory legal acts of the President and Government of the Russian Federation, regulatory documents of the Central Bank of the Russian Federation, the Ministry of Finance of the Russian Federation, and other Federal Executive authorities. Observing the absolute priority of the interests of insured citizens, VEB invests pension savings in order to ensure their growth with a minimum level of risk. Up-to-date VEB manages the funds of about 39 million future pensioners. A state-owned management company invests in government securities, international bonds, deposits, etc.

Isn’t it limited? We consider infrastructure bonds to be of an interest to public authorities in contemporary economic environment.

Currently, there are about 58 non-state pension funds operating in Russia: 36 funds carry out mandatory pension insurance and 18 funds (2.6 trillion rubles).

The allocation of pension reserves and investment of pension savings are based on the following principles:

- ensuring the safety of the funds;
- ensuring profitability, diversification and liquidity of investment portfolios;
- defining an investment strategy based on objective criteria that can be quantified;
- accounting for the reliability of securities;
- information openness of the process; and
- professional management of the investment process and their control.

We consider that pension funds can contribute greatly to the implementation of the environment protection policy by developing financial instruments for sustainable development.

In a contrast to developed countries pension savings legislation in Russia strictly defines the procedure of investment. Russian clients usually choose conservative strategies, the yield of which is less volatile. More than half of investments are accumulated in Russian bonds. However, over the past two years, shareholders ' appetite for risk has increased – the shares of equity and mixed investment funds assets have increased significantly due to net inflows, as well as outperforming returns from investing in shares.

A significant amount of investment by pension funds is concentrated in the Russian oil and gas sector. For example, last year two large associations of private funds were completed: in the middle of the year, three NPFs that fell within the perimeter of the Bank 'FC OTKRITIE 'merged on the basis of 'LUKOIL-Garant' (now NPF 'OTKRITIE'), and at the end of the year 'Consent OPS' and 'Neftegarant NGO' joined the Fund 'Neftegarant'. OTKRITIE NPF with assets at the beginning of this year of 565 billion rubles occupied the second place, but in the first quarter it fell to the third place (market assets decreased to 556 billion rubles), losing to Gazfond Pension savings (563.7 billion rubles). NPF Neftegarant took the ninth place (205.6 billion rubles).

The Association of private funds has also continued its activity. In the first quarter, NPF Safmar was joined by the Trust Fund. As a result, the unified Fund (264.7 billion rubles of assets) in the first three months of the year came in sixth place, ahead of NPF 'Future' (256.5 billion rubles). As a result the concentration of the top 10 Russian private funds exceeded 90% of the reserves

and savings market. The Russian financial market has long been living in a phase of oligopoly. At the beginning of last year, the top 10 players had more than 92.4% of all pension savings. This figure is 2.6 percentage points higher. The non-state pension provision (NGO) market is more diversified, but it is also approaching an oligopolistic one. At the beginning of the year, the ten largest players concentrated 89.5% of all pension reserves.

These examples vividly depict volatility of the Russian financial market and the tendency of oligopolistic accumulation economic capital of institutional investors as participants of financial markets in strategic sectors of the national economy. At the same time, there is a variety of types of II and their instruments, which can contribute to the sustainable development of the national economy. International experience in this regard is taken into consideration.

## Conclusion

The results obtained allowed us to draw the following conclusions. There are several trends for institutional investor's activity in the financial market. Such as growing competition; passive portfolio management strategies with the predominance of active strategies and demand for new investment instruments to form securities portfolio and to manage risks.

The trend of growing competition is supported by increasing regulation requirements for the volume of funds and structure of assets, as well as the constant growth in the number of mutual funds, offering similar services to the population. At the same time, the development of passive strategies is a logical result of continuation, taking into account the changing global environment.

There are also some specific challenges for each type of institutional investors that are determined by market activity of insurance companies, non-state pension funds, and collective investment institutions. Main challenge for the insurance companies is the reduction of insurance schemes (tax optimization) and non-state pension funds activity. As one of the elements of scientific foresight, forecasting allows you to display possible scenarios for the development of institutional investors in Russia. Current market environment has proved, that the authorities are not interested in the development of domestic non-bank financial intermediaries that prevents from transforming savings to investments.

Actually, the activity of institutional investors in the Russian financial market is insignificant. The main share of investments is accumulated by the Federal loan bonds and deposits in leading Russian banks. At the same time,

based on the analysis of investment strategies and market behaviour of key players, we can conclude about passive investment strategies in the Russian financial market. All of the above do not contribute to increasing the role of indirect financing. In order to ensure the security of the Russian financial market, it seems appropriate to take the following measures, which contribute to sustainable economic growth:

- improve taxation of insurance companies, requirements for the structure of the insurance company's investment portfolio and legislation by creating a unified code of responsible investments;
- promote cooperation between insurance companies and management companies, as well as increase information transparency of non-state investment funds.
- clarify the rights of depositors and participants in non-state investment funds while using corporate pension programs.

The above mentioned measures enlarge financial resources to support national programs for sustainable economic development and develop the role of institutional investors in the national economy.

## References

Bernow S., R. Nuttall, S. Brown 2020. Why ESG is Here to Stay. McKinsey & Co. Podcast. 26 May. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/why-esg-is-here-to-stay

Brayley R., S. Myers 2023. *Principles of Corporate Finance.* McGraw Hill.

Eccles R., 21 May 2019. Why It's Time to Finally Worry about ESG. *Harvard Business Review* IdeaCast/Episode 663. https://hbr.org/podcast/2019/05/why-its-time-to-finally-worry-about-esg

Falk R., K. Wang, T. Morris, E. Chan 2023. Environmental Impact and Outperformance: A Data-driven Approach to Integrating Carbon Footprinting into the Investment Process. S&P Global. Market Intelligence. May. https://www.spglobal.com/content/dam/spglobal/mi/en/documents/general/Environmental-Impact-and-Outperformance.pdf

Jacobs, K., J. Robey, K. van Beaumont, C. Lago, M. Rietra, S. Hewett, J. Buvat, N. Manchanda, S. Cherian, B. Abirami 2022. *Consumer Products and Retail. How Sustainability is Fundamentally Changing Consumer Prefe-*

*rences.* Capgemini Research Institute.
Kordsachia, O. 2023. A Risk Management Perspective on CSR and the Marginal Cost of Empirical Evidence from Europe. *Review of Managerial Sciences* April. https://doi.org/10.1007/s11846-020-00392-2
Subramanian S., M. Kabra, S. Chopra, P. Strzelinska, L. Huang, 25 November 2022. ESG Matters – Global. ESG from A to Z: A Global Primer. Bank of America, Merrill Lynch.

Dr. Prof. Irina Yarygina
Moscow State Institute of International Relations
Moscow
Russia
jiz4@yandex.ru

Dr. Vladimir Smirnov
Financial University under the Government of the Russian Federation
Moscow
Russia
vdsmirnov@fa.ru

# Chapter 15: India's Energy Security Vulnerabilities: Assessing Threats to Critical Offshore and Onshore Energy Infrastructure in the Indian Ocean

**Gargi Sharma**
**ORCID iD: https://orcid.org/0009-0007-3046-5019**

> Millenniums before Columbus sailed the Atlantic and Magellan crossed the Pacific, the Indian Ocean had become a thoroughfare of commercial and cultural traffic.
> (Sardar Kavalam Madhava Panikkar)

## Abstract

This chapter is a study of what India has categorised as Offshore Development Areas (ODAs) in its Exclusive Economic Zone, to explore and exploit these resources for economic gains. A number of private as well as state-owned companies have set up their installations in these ODAs for this purpose. On the one hand, the great waters serve as a gateway to prosperity in the form of trade and commerce opportunities, but on the other hand, they also pose a serious challenge to the peace and security of the country. In the context of this chapter, 'Energy Security Vulnerabilities' are defined as the susceptibilities and threats that compromise the stability, integrity, and safety of energy resources and infrastructure. These vulnerabilities encompass a range of non-traditional threats such as maritime terrorism, piracy and armed robbery which have been on the rise in the maritime space in the last few decades and can be attributed to the ignorance of littoral states as well as maritime law enforcement agencies towards maritime security (also known as 'sea blindness'). Perceiving maritime space as an extension of their theatre of operations, the illicit non-state actors such as maritime terrorists, pirates and armed robbers have been making good

use of this sea blindness and targeting offshore assets including critical energy infrastructure as well as vessels for nefarious financial and political gains.

**Keywords:** Energy dependency, critical energy infrastructure, energy security vulnerabilities, offshore energy infrastructure, onshore energy infrastructure, sea blindness

## 1 Introduction

Sardar K.M. Panikkar, a distinguished Indian statesman, diplomat, and scholar who significantly influenced India's foreign policy and its understanding of international relations during the early years of independence, reaffirmed the importance of the Indian Ocean for the Indian subcontinent in his work 'India and the Indian Ocean'. India has traditionally been a maritime nation (Muralidharan 2021). The subcontinent's maritime legacy dates back thousands of years. With a long coastline of more than 7,500 kilometres, nine states situated along the coast and millions depending upon maritime sector, the sea plays a key role in India's economy even today. Having nearly two-third of its borders surrounded with water and over 95% of the trade being carried out via sea routes, India's dependence over its waters is fairly high. Owing to the expansive baseline, the country is fortunate to possess an Exclusive Economic Zone (EEZ) of nearly 2.7 million sq km. This EEZ contains a number of energy and natural resources, including oil, gas and coal.

India has categorised Offshore Development Areas (ODAs) in its Exclusive Economic Zone to explore and exploit these resources for economic gains and a number of private as well as state owned companies have set up their installations in these ODAs for this purpose. On the one hand, the great waters serve as a gateway to prosperity in the form of trade and commerce opportunities, but on the other hand, they also pose a serious challenge to the peace and security of the country. In the context of this chapter, 'Energy Security Vulnerabilities' are defined as the susceptibilities and threats that compromise the stability, integrity, and safety of energy resources and infrastructure. These vulnerabilities encompass a range of non-traditional threats such as maritime terrorism, piracy and armed robbery which have been on the rise in the maritime space in the last few decades and can be attributed to the ignorance of littoral states as well as maritime law enforcement agencies towards maritime security (also known as 'sea blindness'). Perceiving maritime

space as an extension of their theater of operations, the illicit non-state actors such as maritime terrorists, pirates and armed robbers have been making good use of this sea blindness and targeting offshore assets including critical energy infrastructure as well as vessels for nefarious financial and political gains.

## 2 Critical Energy Infrastructure

As per Resolution 2341 (2017) of the United Nations Security Council, the Critical infrastructure has to be determined by the state itself based on its own priorities and interests. It may cover communications; energy; finance; food; public services; industry; health; transport; gas; radio and television; information technology; commercial facilities; chemical and nuclear sectors; and water. The European Union's report on Migration and Home Affairs defines the Critical infrastructure as an 'asset or system which is essential for the maintenance of vital societal functions'[1]. It is not an easy task to determine 'criticality' of specific sectors due to their interdependencies and shift in priorities with time. Detailed judgement and calculation are needed in order to decide the criticality factor (Clemente 2021).

India does not have any organisation or policy solely dedicated to the protection of its critical infrastructure except National Critical Information Infrastructure Protection Centre (NCIIPC) established by the Government of India in 2015 which deals with protection of Critical 'Information' Infrastructure. This Centre defines Critical Sectors as those 'which are critical to the nation and whose incapacitation or destruction will have a debilitating impact on national security, economy, public health or safety'[2]. They are extremely vital for a country's thriving economy and form an important part of its national identity and strategic purpose. Energy related critical infrastructure located on the coast or even miles away from the mainland serves as easy prey for pirates and terrorists hunting for resources. Critical offshore energy infrastructure found in the ODAs include fixed offshore production platforms (gravity-based structures, GBSs), jacket structures, tension-leg platforms (TLPs), tower platforms), mobile offshore drilling units, FPSOs, FSOs, FDPSOs, offshore oil export terminals, drill ships, jack-ups, submersibles, single point moorings and

[1] European Commission, 'Migration and Home Affairs'.

[2] National Critical Information Infrastructure Protection Centre (NCIIPC), 'Guidelines for Identification of Critical Information Infrastructure'.

other kinds of offshore installations such as oil derricks, wellhead platforms, and flow stations (Kashubsky 2011).

## 3 India's Energy Dependency and Onshore and Offshore Energy Infrastructure (assessing existing regulations and policies)

The Energy sector is of critical importance to sustain the industrial and economic growth of any country. India's energy needs are multifaceted and arise from a diverse mix of sources, reflecting the country's extensive and varied consumption patterns. The primary energy demands in India are met through a combination of fossil fuels, renewable resources, and traditional biomass. According to the International Energy Agency (IEA), coal is the largest source of energy, contributing approximately 55% to the country's energy mix, while oil and natural gas contribute about 30% and 6%, respectively[3]. Additionally, India has made significant strides in the utilization of renewable energy sources, including solar and wind power, which together accounted for around 10% of the total energy consumption as of 2022[4]. The use of biomass, including wood and agricultural residues, remains significant in rural areas, addressing both energy needs and socio-economic development[5]. At the domestic level, energy consumption patterns vary widely, with urban areas relying heavily on electricity and fossil fuels, while rural areas continue to depend more on traditional energy sources. Regionally and nationally, the disparity in energy needs necessitates a nuanced approach to energy policy and infrastructure development, tailored to address both urban and rural demands while promoting sustainability and energy security.

Hence for an energy-deficient country like India, the well-being of energy related infrastructure becomes extremely crucial, since any disruption in this sector can lead to serious impact on the country's growing economy. And this is why energy security is at the core of India's foreign policy approach. The lion's share of India's domestic energy resources is found in the ODAs located in the EEZ, which makes it even more important to ensure safety of offshore assets standing in the seas.

[3] International Energy Agency, 'India Energy Profile'.
[4] Ministry of New and Renewable Energy, Government of India.
[5] United Nations Development Programme, 'Sustainable Energy for All'.

| Total Domestic Oil & Gas Production (as of April 2019) [Source: Ministry of Petroleum and Natural Gas] | | | | | |
|---|---|---|---|---|---|
| **Crude Oil** | | | **Natural Gas** | | |
| Onshore | 20.01MMT | (58.5%) | Onshore | 10.75 BCM | (32.7%) |
| Offshore | 14.19 MMT | (41.5%) | Offshore | 22.12 BCM | (67.3%) |
| Total | 34.20 MMT | | Total | 32.87 BCM | |

The total indigenous crude oil production in FY 2018-2019 was 34.20 MMT metric tonnes, in which offshore accounted for 14.19 MMT. Similarly, 22.12 bil-lion cubic meters out of the total natural gas production of 32.87 billion cubic meters was produced in the offshore area during the same period[6]. In April 2019, the onshore Crude oil recoverable reserves were estimated at 341.33 million tonnes (55%) and the offshore Crude oil recoverable reserves were estimated at 277.60 million tonnes (45%). The largest share of crude oil reserves is owned by ONGC (70%) followed by Oil India Limited (12%) and Private Sector Companies (18%) (Figure 3.1).

Similarly, the onshore natural gas recoverable reserves were estimated at 492.30 billion cu. m (36%) and the offshore natural gas recoverable reserves were estimated at 888.34 billion cu. m (64%). In this case, the largest share of natural gas reserves is owned by Private Sector Companies (50%) followed by ONGC (41%) and Oil India Limited (9%) (Indian Minerals Yearbook 2019)[7].

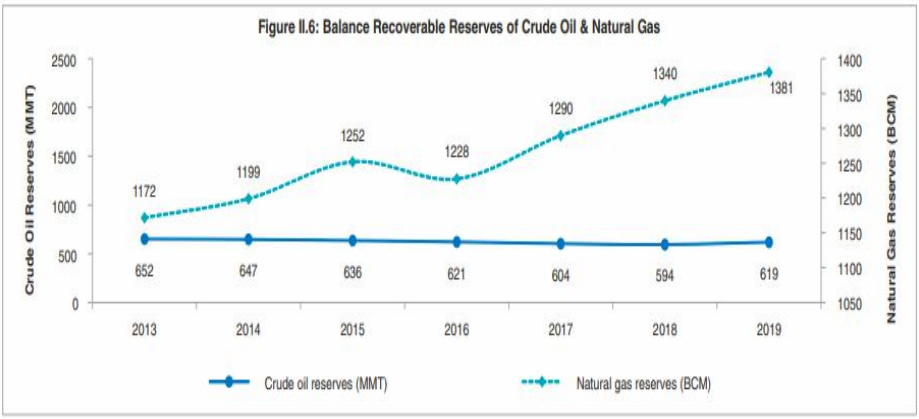



**Figure 3.1 Source: Ministry of Petroleum and Natural Gas, 2018-19**

[6] Ministry of Petroleum and Natural Gas (2020).
[7] Indian Minerals Yearbook (2019).

These statistics indicate India's reliance on offshore fields which constitute a significant part of total crude oil and gas reserves.

| **Balance recoverable reserves (as of April 2019)** [Source: Ministry of Petroleum and Natural Gas] | | | | | |
|---|---|---|---|---|---|
| **Crude Oil** | | | **Natural Gas** | | |
| Onshore | 341.33 MMT | (55%) | Onshore | 492.30 BCM | (36%) |
| Offshore | 277.60 MMT | (45%) | Offshore | 888.34 BCM | (64%) |
| Total | 618.94 MMT | | Total | 1,380.64 BCM | |

Along with the domestic onshore and offshore resources, the country imports a huge amount of the oil and natural gas via International Shipping Lanes across Indian Ocean to meet its energy needs. India also exports refined petroleum and petroleum products to other countries. Considering the 'total oil imports by sea, offshore oil production and petroleum exports, the country's cumulative sea dependence for oil is estimated to be about 93%'[8]. The country seeks to 'encourage domestic and international cooperation with foreign oil and gas companies'' in order to boost the energy drive. Hence, the Indian subcontinent's energy requirement is highly dependent upon seas. The Indian Navy as well as other maritime security agencies are familiar with this sea dependence and are responsible for the protection of fixed and mobile offshore assets and vessels carrying oil and gas, Sea Lines of Communications and coastal areas. India's historical naval defences along these sea routes are already well documented. Over the recent past for instance, their role on averting Houthi and Somalian pirate attacks against this international sea route has produced remarkable results. The Maltese flagged MV Ruen was freed by the Indian Navy after it was hijacked on 23 December 2023, around 700 nautical miles eat of Bosasa. However, the rescue operation only took place in March 2024 after a coordinated effort by several vessels of the Indian navy, who admirably did not have to injure or kill any of the ship's crew or the pirates. The ship's crew of 17 were released and 35 Somalian pirates were taken to a Mumbai court for trial[9].

[8] Ministry of Defence (Navy) (2015).
[9] Defence Web, 'Indian Navy Rescues Another Pirated Ship'.

India's Offshore Energy Infrastructure comprises Western and Eastern Offshore Development Areas (ODAs). The Western ODA includes Mumbai High (North & South), Mukta, Bassein, Neelam, Panna, Tapti, Heera, Laxmi and Gauri whereas the Eastern ODA include Mahanadi, Cauvery and Krishna Godavari basins (Figure 3.2).

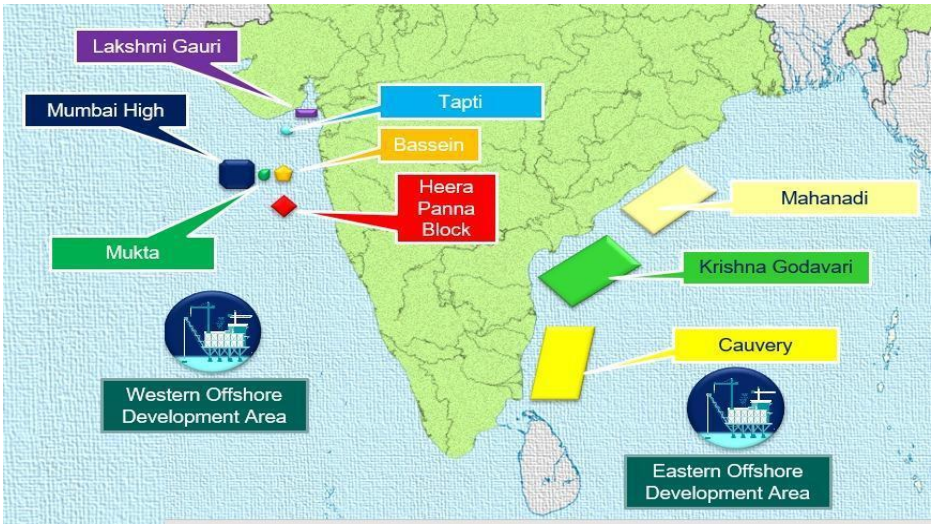



**Figure 3.2 - Western and Eastern ODAs of India**

## 4 Maritime Terrorism

Very few terrorist activities against offshore critical infrastructure have been reported in the past, largely due to underreporting or lack of sufficient skills and technology owned by terrorist organizations. But with time, they have evolved and became inventive, resourceful and more advanced in technological terms. These non-state actors now possess some of the advanced and state-of the art technology (incl. GPS and satellite communications) and weaponry; and a number of skilled professionals joining these terrorist organisations makes the threat imminent in the near future. They seek to deliberately create disturbance, exploit vulnerabilities and constantly search new targets to spread fear as well as disrupt the smooth functioning of an economy. Critical Infrastructure serves their purpose quite well, as it has the ability to directly impact the economy with the minimal risk of being caught.

In the past few years, there have been many cases where terrorist groups have targeted energy infrastructure in several countries. The most recent ones have been a series of missile and drone attacks on the oil facilities of world's biggest oil exporter Saudi Arabia's oil giant, Aramco by the neighbour Yemen's Houthi rebels. In September 2019, two Saudi oil refineries Abqaiq and Khurais were attacked, which resulted in production halt and prolonged disruption. In March 2021, an oil storage yard at Ras Tanura, the site of an oil refinery and the world's biggest offshore oil loading facility was attacked with the intention of targeting the 'security and stability of global energy supply' (Al Jazeera 2021). If Yemen's Houthis were able to carry out such advanced drone attacks against energy infrastructure, the other terrorist organizations in India's neighborhood, such as Jaish-e-Mohammed (JeM), based primarily in Pakistan-administered Kashmir; Lashkar-e-Taiba (LeT), also based in Pakistan; and the Liberation Tigers of Tamil Eelam (LTTE), based in Sri Lanka, could potentially carry out similar attacks.

Gujarat, with its highly vulnerable 1,600-km porous coastline, hosts installations of vital economic significance (Hiral 2009). It has the longest coastline among all Indian states. The Gulf of Kutch in the state houses two major oil ports, Mundra and Kandla which lie in close vicinity of Pakistan.

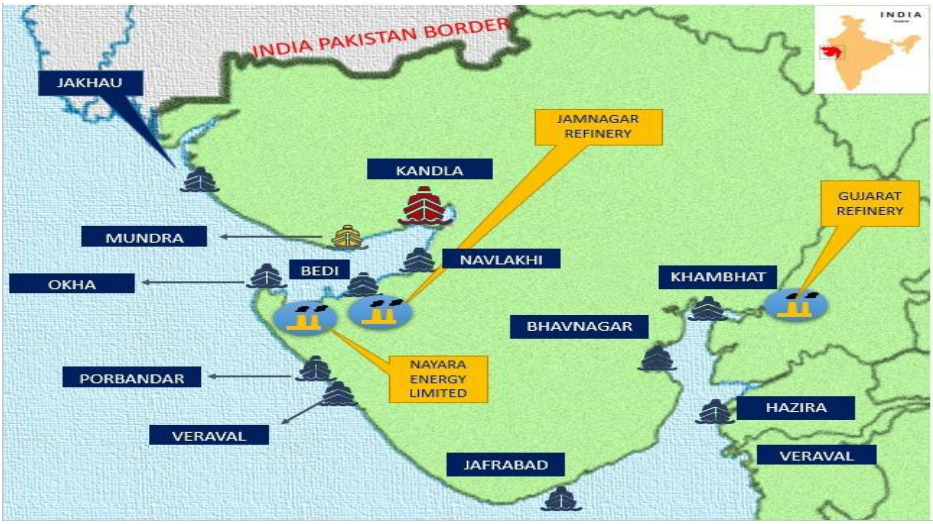



**Figure 4.1 Gujarat - Significant ports and refineries**

Mundra is one of the largest ports in the country run by Adani group, whereas Kandla port is a large bulk handling facility.

Most of India's oil imports are sourced from Persian Gulf, and Gujarat's ports serve as the closest points. Kutch region also includes *Reliance Industries*' Jamnagar oil refinery (50 million-tonne) which is the largest in the world and the Nayara Energy Refinery (formerly *Essar Refinery*) at Vadinar (11 million-tonne) followed by Gujarat Refinery. With so many critical installations in one place, the Kutch is clearly a highly sensitive region or rather a 'gunpowder keg' of the country (Unnithan 2001). Any attack on any of these installations in the same fashion as conducted by Houthis on Saudi Aramco in 2019 can be disastrous for the Indian energy industry.

Terrorism is not going to end anytime soon and India, with its strong stand against any kind of terrorist activities, stands in the category of foe and may fall prey to their vicious tactics. The country has witnessed several terrorist attacks in the past, and one of them was seaborne. The brutal 26/11 attacks, which brought the Indian city 'which never sleeps' (Mumbai), to a standstill in 2008, are still fresh in the national consciousness. The Mumbai attacks planned and executed by Lashkar-e-Taiba were launched from Karachi and became successful due to the shortcomings of the then maritime security architecture. The growing presence of some terrorist organisations including ISIS and Al Qaeda in neighbouring countries and attacks on naval installations including PNS Mehran (2011), PNS Zulfiqar (2014), and Chittagong (2015) not too far from the Indian borders pose serious threats to the country's maritime security.

Offshore energy installations, particularly, oil and gas infrastructure, are scattered all over the EEZ and are more vulnerable and hardly defensible targets due to their remoteness. Hence they tend to be a more attractive target for illicit non-state actors. Oil, due to its high demand and dependency, serves as the Achilles heel of the country's economy. In 2011, there were reports of a new terror plot being planned by the terrorist groups Lashkar-e-Taiba and Jaish-e-Mohammed. It was suspected that they were going to hit India's offshore oil installations by detonating explosive laden ships.

Such a possibility by terrorists now looms large against Indian energy facilities. Attacking the country's offshore structures can prove to be fatal for the energy-dependent economy and will be a prize attack for India's enemies. A number of methods, including explosives in suicide boats or light aircraft, unmanned submarine bombs, and/or ship-launched missiles are possible. Attacks on offshore energy installations cause infrastructural and environmental damage as well as production halt. This leads to productivity and consequential

financial losses, price rises and market fluctuations. Ultimately all these factors contribute towards reduced confidence in the country's existing security measures and affect geopolitics and foreign relations negatively. The Limburg bombing (2002) can be a perfect example because it caused considerable consternation among the global and Yemeni shipping community and impacted global oil trade negatively.

# 5 Responses and Coordination at International, Regional and National Levels

This section explores the multifaceted responses and coordination mechanisms employed at international, regional, and national levels to enhance maritime security. We will begin with an examination of India's maritime security architecture, focusing on coastal and offshore security measures, capability and capacity development, and the intricacies of maritime domain awareness and information sharing networks within the Indian Ocean. Understanding these elements is crucial, as they reveal how national strategies align with broader regional and international frameworks. Following this, we will delve into the United Nations Convention on the Law of the Sea (UNCLOS) of 1982, which establishes the legal foundation for maritime conduct and cooperation, and the International Maritime Organization (IMO), which plays a pivotal role in setting global maritime standards and regulations. By examining these international and regional frameworks alongside India's national strategies, we aim to provide a comprehensive overview of how different layers of governance and coordination contribute to maritime security. This approach underscores the interconnectedness of national defense strategies with international maritime laws and organizations, highlighting their collective impact on enhancing maritime security.

## *5.1 India's Maritime Security Architecture*

Maritime Security comprises security on land as well as sea, therefore it is a complex construct. It requires coordinated efforts from all maritime stake-holders including Indian Navy, Coast Guard, port authorities, and the local community. Moreover, unlike the land borders which can be easily demarcated, the maritime boundaries cannot be demarcated. After the 26/11 Mumbai attack, the existing maritime security structure was restructured to a large extent.

Following the attacks, the Indian government led by Prime Minister Manmohan Singh, in collaboration with the Indian Navy, Coast Guard, and other agencies, embarked on an extensive restructuring of maritime security. New assets, including patrolling vessels, aircrafts and better weapons were acquired[10]. The existing technological infrastructure was upgraded and funding for better technologies such as Automatic Identification System and coastal radars was approved. The funding and approval for these enhancements were part of a broader initiative spearheaded by the Indian Ministry of Defence in collaboration with the Bharatiya Janata Party (BJP) government, which emphasized a comprehensive approach to maritime safety[11]. Enhanced monitoring, detection and identification measures were introduced for local fishermen and traders. And most importantly, maritime security became the joint responsibility of the three-tier cordon Indian Navy, Coast Guard and marine police as well as maritime intelligence agencies and port authorities. And this may be the reason why there has not been a single seaborne terrorist attack after the 26/11 incident (Karve 2018). The authorities responsible for the security of maritime space and borders have become more cautious about the safety of overall maritime space.

- ***Coastal and Offshore Security***

## Indian Navy

- Flag Officer Defence Advisory Group: The Flag Officer Defence Advisory Group (FODAG) is responsible for the safety of all offshore assets. The FODAG was set up in 1983 in order to ensure the security of Offshore Development Areas. It is chaired by the Flag Officer (Rear Admiral) of the Indian Navy and acts as nodal agency to advise all the companies involved in the offshore exploration and production activities concerning security measures. Headed by the DG (Indian Coast Guard), the 'Offshore Security Coordination Committee' (OSCC) works in coordination with FODAG to ensure the safety. It is also responsible for offshore security of the country. Along with these two groups, the third committee which is responsible for

[10] Ministry of Defence, 'After 26/11, What Steps Have Been Taken to Strengthen the Intelligence System and Surveillance?'

[11] Press Information Bureau, Government of India, Ministry of Defence, 'Initiatives to Strengthen Coastal Security'.

the offshore infrastructure protection is Regional Contingency Committee chaired by the Chief of Staff of Western and Eastern Naval Commands of Indian Navy.

- Exercise 'PRASTHAN*':* This is a joint exercise conducted by the Eastern as well as Western Naval Command of the Indian Navy as part of Crisis Management Group with other maritime stakeholders every six months on offshore installations[12]. It is carried out every six months by Marine Commandos (MARCOS) and Explosive Ordinance Disposal (EOD) of the Indian Navy in the form of mock drills to assess the preparation of security agencies to safeguard ODAs and prevent potential contingencies such as asymmetric threat or terrorist action, oil spill, casualty evacuation and fire.

- Exercise 'SEA VIGIL'*:* In 2019, the Indian Navy conducted the 'largest coastal defence exercise' named SEA VIGIL[13]. It was carried out along the country's entire coastline and EEZ and was aimed at demonstrating the effectiveness of the steps undertaken post Mumbai attacks in 2008 and securing ODAs as well as energy related assets including SPMs and support vessels. One of its objectives was the assessment of critical zones and identification of shortfalls in the maritime security architecture (Das 2020). The timing of this exercise, occurring 11 years after the Mumbai attacks, can be attributed to several factors, including the gradual development of enhanced maritime security frameworks and the need for comprehensive assessment and preparation to address evolving threats. The extended period reflects the complexity of implementing and testing a robust security infrastructure across such a vast maritime domain.

## Indian Coast Guard

- The Indian Coast Guard is responsible for the coastal as well as offshore security. It conducts round the clock patrolling by means of fast patrolling vessels as well as aerial surveillance with the help of shore-based aircraft

[12] 'Exercise Prasthan Conducted in Western Offshore Development Area Under Aegis of the Western Naval Command, Mumbai'.
[13] 'Indian Navy Coordinates Largest Ever Coastal Defence Exercise Ten Years After 26/11'.

and helicopters in the Indian EEZ. The aircrafts owned by Indian Coast Guard have advanced sensors to detect unlawful activities and weaponry to prevent them. Set up in 1987, the 'Offshore Security Coordination Committee' headed by the DG (Indian Coast Guard) plays a key role in strengthening maritime security measures along with FODAG and RCC[14].

- ***Capability and Capacity Development***

In the last few years, the institutions responsible for the security of the nation have begun prioritising capability building over capacity building, although the latter has also not been ignored. Capacity building refers to increasing the quantity and availability of resources, such as acquiring equipment or personnel. After the 26/11 attack, the authorities approved the acquisition of numerous patrol boats for the marine police to enhance their presence in the territorial waters. However, capability building, which involves developing the skills, training, and operational effectiveness of personnel, was insufficiently addressed. The marine police lacked the necessary training to operate these boats and were unfamiliar with maritime borders, leading to the underutilization of the new assets. Security agencies have since recognized the importance of both capacity and capability development. Therefore, it is crucial that security personnel receive proper training in conjunction with the provision of equipment to ensure that resources are effectively utilized.

- ***Maritime Domain Awareness and Information Sharing Network in Indian Ocean***

Failure to locate and recognise the potential threats can lead to disastrous results, hence Maritime Domain Awareness (or MDA) is a significant step towards improving and encouraging coordination among regional partners. It was one of the major initiatives undertaken after the Mumbai attack to develop a system for identification and tracking of vessels and fill gaps in the maritime domain. It included coastal mapping, satellite-based tracking system and vessel traffic service (Das 2020). The objective of an information sharing network is establishment of protocols to share sensitive data related to critical installations in the maritime domain and assessment of data requirements. During IORA's inaugural summit in 2017, India announced its decision to enhance international

[14] 'Maritime Surveillance', Indian Coast Guard.

Maritime Domain Awareness in the region. The Information Fusion Centre-IOR was set up in Gurugram in 2018 by the Indian Navy with the objective to combat maritime terrorism, piracy and other safety-related challenges.

- ***Coastal Border Management***

After the 26/11 attacks, the Government of India, under the leadership of Prime Minister Manmohan Singh, along with the Indian Navy and Coast Guard, introduced several initiatives in 2009 to strengthen India's coastal security architecture, including coastal security scheme, national automatic identification system, vessel tracking management systems, coastal surveillance network, and community interaction programs. The porous creeks on the coasts of Sundarbans in West Bengal and Gulf of Kutch in Gujarat are the most difficult terrains to secure. They have a 'maze of channels which weave in and out of international borders' (Kamat 2019). The sandbars, mangroves and numerous islands serve as the best hideaways for the intruders. Hence it is important to have non-stop maritime border patrols. Even the huge EEZ area is difficult to patrol and poses a threat of infiltration. The security agencies make good use of technology, surveillance and communication to keep the area safe.

## 5.2 United Nations Convention on the Law of the Sea 1982

The United Nations Convention on the Law of the Sea (1982) provides a set of regulations for coastal states on the issues related to the rights, responsibilities and jurisdictions in the seas. It also provides a safety protocol for the offshore infrastructure of the coastal states located in the Exclusive Economic Zone (EEZ) which is located within 24 to 200 nautical miles of the baseline. The Article 56 of the Convention states that the coastal states have 'sovereign rights' to establish installations in the EEZ for the economic exploitation and exploration of the zone[15]. However, it is important to note that establishment of offshore installations does not change the legal status of surrounding waters.

According to Article 60, the coastal states may create 'a safety zone around the installation', however it 'shall not exceed a distance of 500 metres, except as authorized by generally accepted international standards or as recommended by the competent international organization'. The UNCLOS also

[15] 'United Nations Convention on the Law of the Sea (UNCLOS), United Nations.

informs the vessels to 'respect these safety zones'. The agencies of the coastal state responsible for the safety of offshore infrastructure are entitled to take preventive measures and even use force in case of violations or infringements in order to ensure the security. If they feel that there is a potential threat to any infrastructure, they may choose to temporarily suspend the 'right to innocent passage' of foreign vessels.

The concept of a safety zone, established nearly four decades ago, was originally intended to mitigate 'navigational hazards' rather than address deliberate and planned threats (Williams 2014). In the maritime domain, a 500-meter safety zone is inadequate to 'operate defensive tactics'. For instance, a suicide bomber aboard an explosive-laden vessel could reach and impact a target within 30 to 40 seconds, rendering it extremely difficult for even the most well-prepared security teams to detect, communicate, and respond in time. Consequently, there is an urgent need to reassess and extend the safety zone to better counter contemporary threats.

In order to avoid any navigational mishappenings, the Indian Ministry of Ports, Shipping and Waterways released a Merchant Shipping Note and established the safety fairways in 2008 for all Indian (mandatory to follow) and foreign (recommended) vessels passing through Western ODA within India's EEZ. Along with this, it also established recommended routes along Gujarat coast to regulate coastal traffic and to keep the passing vessels away from ODAs[16]. In 2009, when the Intelligence Bureau alerted the intelligence agencies that terrorist organisations based in Pakistan were planning to execute attacks on Indian offshore oil and gas installations, the Government of India took into consideration the plan to extend the safety zone breadth from 500 meters to 5 nautical miles which could help the responsible security agencies to improve the security measures and prevent any sabotage or terrorist attacks. Unfortunately, the plan did not materialise (Anupama Airy 2009).

## 5.3 International Maritime Organization

IMO takes an active part in the counter-terrorism and capacity building coordination activities under the aegis of UNSC counter-terrorism Committee and UNGA Counter Terrorism Implementation Task Force[17]. Resolution

[16] National Hydrographic Office, 'Indian Notices to Mariners'.

[17] 'The Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices'.

A.671(16), adopted by the International Maritime Organisation in 1989 recommends a number of preventive measures, if the safety zone regulation is violated. However, this resolution isn't binding. It is up to the states to follow or not follow the measures, hence the coastal states are not entitled to take any enforcement actions against the states or their vessels.

No approval to extend the safety zone has been given by IMO so far. Although some coastal states have extended the safety zone limit by virtue of their domestic legislation, especially if the offshore installations consist of floating production storage and offloading units (FPSOs) and/or floating storage and offloading units (FSOs) (Kashubsky & Morrison 2013). Nigeria for instance has a safety zone of 3 miles around its Pennington Offshore Terminal. The foreign vessels are not allowed to enter the zone, however they are not legally bound to follow the extension rule.

- ***Regional Cooperation and Coordination***

The IMO conducts a number of national and regional Programs by means of its several activities promoting technical cooperation and capacity building. Its Global Maritime Security Programme seeks to assist the states in identification and compliance of its legal frameworks. It attempts to bring the states together and establish an international framework to enhance cooperation between them in identifying threats to offshore infrastructure. IMO recommends the adoption of a 'risk based preventive strategy' against terrorist attacks on ports and maritime structures.

- ***Training, Capacity Building and Information Sharing***

IMO ensures the protection of Critical Infrastructure against terrorism as part of its initiatives to secure the civil maritime industry. It has 'developed a range of guidance, self-assessment tools and training materials for the protection of ports, ships and offshore installations. As threats have evolved, IMO's focus on reactive efforts to counter terrorism has been replaced by an emphasis on proactive measures'[18]. Traditionally the protection of maritime infrastructure has been the responsibility of particular agencies instead of any multilateral

[18] United Nations, 'Security Council Calls on Member States to Address Threats against Critical Infrastructure, Unanimously Adopting Resolution 2341 (2017)'.

institution. IMO seeks to improve maritime security by conducting activities promoting capacity building in the developing nations and building an information-sharing network[19].

## 6 Recommendations for India

- ***Need of Efficient Risk Management Framework***

The majority of energy infrastructure in India is owned by private companies including Reliance and Essar. In the last 3-4 decades, they have sufficiently invested in security strengthening and risk management to follow safety protocols and maintain consumer confidence. However, the threats have evolved with time and it has now become crucial for the private sector to join hands with the security agencies and reassess and upgrade the existing framework.

- ***Enhancing Cross-border Cooperation Initiatives***

India should collaborate with its neighbours to implement cross-border initiatives in the field of offshore critical energy infrastructure protection by sharing necessary security-related information and adopting a collaborative approach to prevent maritime terrorism. It may include sharing the information related to vessels of fishermen and local traders or patrolling the maritime borders.

- ***Enhancing International and Regional Cooperation***

The importance of understanding that terrorism and the malicious intentions of illicit non-state actors are not confined to the boundaries of the countries cannot be overstated. It is very crucial to come together and join hands against this evil and save humanity. The member states of some international organisations like European Union have designed frameworks and policies to coordinate the security of critical energy infrastructure against non-state actors. India should call upon international organisations such as IORA, IPOI, BIMSTEC and BRICS to come together to strengthen security measures with regard to critical energy infrastructure.

[19] 'Compendium of Good Practices'.

- ***Strengthening/ Suggesting Regulations and Policies***

In 2009, the request for extension of the safety zone was considered by IMO, but it was not approved[20]. Considering contemporary threats and scenarios with international terrorism, the safety zone boundary should be extended to at least 2 nautical miles. Since India is situated in a high-risk area of the world its safety zone must be extended from 500 meters to anything between 2-5 nautical miles in order to ensure their safety. This is very possible since the IMO states that extensions can be done '… on a case-by-case basis .. upon request of the coastal State'.

## Conclusion

Unlike land boundaries, maritime borders cannot be effectively secured with artificial barriers and walls. Despite constant vigil and dedicated efforts, vast oceans and inadequate resources make it difficult for the three-tiered cordon to conduct patrolling and surveillance. The offshore and onshore energy infrastructure is highly critical to the economy and ecology of the country, therefore proactive consideration must be given to its protection by the policymakers and new policies must be developed with the urgency it deserves, so that any future attacks can be prevented (Blackmon 2020). Instances like 2019 Houthi attacks on Saudi Arabian oil facilities underscore the evolving threat landscape and the potential impact on critical infrastructure. The non-state actors' technological advancements and gradual shift of focus from land to sea is alarming and the tendency of neglecting potential maritime threats will gravely impact national security. Hence it is imperative to focus seawards, adopt a comprehensive approach and face the adversaries propagating in the sea with better organised counter-terrorism strategies.

## References

Al Jazeera 2021. Fire at Saudi Arabia Oil Facility after Drone Attack. (Accessed on 18 February 2021.) https://www.aljazeera.com/news/2021/3/19/fire-at-saudi-arabia-oil-facility-after-drone-attack

Anupama Airy, 16 November 2009. Govt to Secure Offshore Oil and Gas Installations. *Hindustan Times*. (Accessed on 07 March 2021.)

[20] International Maritime Organization (2009).

https://www.hindustantimes.com/business/govt-to-secure-offshore-oil-and-gas-installations/story-gDLSFgT3qJTft96oMU6spK.html

Blackmon, D. 2020. Piracy Attacks on Oil Facilities and Vessels: An Issue the U.S. Could Soon Face. Forbes. (Accessed on 21 February 2021.) https://www.forbes.com/sites/davidblackmon/2020/11/15/piracy-attacks-on-oil-facilities-and-vessels-an-issue-the-us-could-soon-face/?sh=623053f87734

Captain Himadri Das, 01 December 2020. Coastal Security in India: Twelve Years After '26/11'. National Maritime Foundation. (Accessed on 17 February 2021.) https://maritimeindia.org/coastal-security-in-india-twelve-years-after-26-11/

Captain Himadri Das, 23 March 2021. An Integrated Approach to Coastal and Offshore Defence: Leveraging the Coastal Security Construct. National Maritime Foundation. (Accessed on 24 March 2021.) https://maritimeindia.org/an-integrated-approach-to-coastal-and-offshore-defence-leveraging-the-coastal-security-construct/

Clemente, D., February 2013. Cyber Security and Global Interdependence: What Is Critical?. *Chatham House*. (Accessed on 15 February 2021.) https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf

Compendium of Good Practices 2023. United Nations Security Council Counter-Terrorism Committee. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/eu_un_compendium_good_practice_web.pdf

Curran, 23 May 2019. Soft Targets & Black Markets: Terrorist Activities in the Maritime Domain. *Stable Seas*. (Accessed on 15 February 2021.) https://www.stableseas.org/publications/maritime-terrorism/soft-targets-black-markets-maritime-terrorism

Defence Web, 'Indian Navy Rescues Another Pirated Ship'. (Accessed on 14 September 2024.) https://www.defenceweb.co.za/african-news/indian-navy-rescues-another-pirated-ship

European Commission. Migration and Home Affairs. https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/protection_en (Accessed on 15 February 2021.)

Exercise Prasthan Conducted in Western Offshore Development Area Under Aegis of the Western Naval Command, Mumbai, December 2023. Indian Navy (Accessed on 12 February 2021.)

https://www.indiannavy.nic.in/content/exercise-prasthan-conducted-western-offshore-development-area-under-aegis-western-naval

Hiral, D., 17 September 2009. 1,600-km Porous State Coastline Still Vulnerable. *The Indian Express*. (Accessed on 15 March 2021.) https://indianexpress.com/article/cities/ahmedabad/1-600km-porous-state-coastline-still-vulnerable/

Indian Minerals Yearbook 2019. (Part-III: Mineral Reviews), Indian Bureau of Mines, Ministry of Mines, Government of India. (Accessed on 15 February 2021.) https://ibm.gov.in/writereaddata/files/11092020132633PNG_2019.pdf

Indian Navy. Flag Officer Defence Advisory Group: Historical Background. (Accessed on 28 February 2021.) https://www.indiannavy.nic.in/content/fodag-0

Indian Navy Coordinates Largest Ever Coastal Defence Exercise Ten Years After 26/11, 22 January 2019. Press Information Bureau, Government of India, Ministry of Defence (Accessed on 28 February 2021.) https://pib.gov.in/Pressreleaseshare.aspx?PRID=1560995

Indian Navy, Department of Defence, Ministry of Defence. (Accessed on 12 February 2021.) https://www.mod.gov.in/dod/faq

International Maritime Organization, Sub-Committee on Safety of Navigation (NAV). 55th Session 2009. (Accessed on 15 February 2021.) https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/NAV-55th-session.aspx

Kamat, P.V., 11 July 2019. India's Coastal Security: Perspectives, Challenges and Prospects. *FINS Journal of Diplomacy & Strategy*. (Accessed on 03 March 2021.) https://finsindia.org/journal/indias-coastal-security-perspectives-challenges-and-prospects/

Kashubsky, M. 2011. Offshore Petroleum Security: Analysis of Offshore Security Threats, Target Attractiveness, and the International Legal Framework for the Protection and Security of Offshore Petroleum Installations, PhD dissertation, University of Wollongong.

Kashubsky, M. & A. Morrison 2013. Security of Offshore Oil and Gas Facilities: Exclusion Zones and Ships' Routeing. *Australian Journal of Maritime and Ocean Affairs* 5,1: 2 – 7. https://static.s123-cdn.com/uploads/3635447/normal_5ee1a6d0370e4.pdf; https://doi.org/10.1080/18366503.2013.10815725

Maritime Surveillance. Indian Coast Guard. (Accessed on 24 March 2021.) https://www.indiancoastguard.gov.in/content/1718_3_MaritimeSurveillance.aspx

Ministry of Defence (Navy) 2015. Ensuring Secure Seas: Indian Maritime Security Strategy. (Accessed on 15 February 2021.) https://indiannavy.nic.in/sites/default/files/Indian_Maritime_Security_Strategy_Document_25Jan16.pdf

Ministry of Defence. After 26/11, What Steps Have Been Taken to Strengthen the Intelligence System and Surveillance? (Accessed on 12 September 2024.) https://mod.gov.in/faqs/q-6-after-2611-what-steps-have-been-taken-strengthen-intelligence-system-and-surveillance

Ministry of New and Renewable Energy, Government of India 2022. Annual Report 2022. (Accessed on 12 September 2024.) https://mnre.gov.in/annual-report-2022

Ministry of Petroleum and Natural Gas, 2020. Monthly Production Report. (Accessed on 22 March 2021.) http://petroleum.nic.in/sites/default/files/MPRjanuray20.pdf

National Critical Information Infrastructure Protection Centre (NCIIPC) 2015. Guidelines for Identification of Critical Information Infrastructure. (Accessed on 15 February 2021.) https://nciipc.gov.in/documents/Guidelines_for_Identification_of_CII.pdf

National Hydrographic Office, Indian Notices to Mariners. (Accessed on 25 February 2021.) http://intmsearch.gov.in/bimonthly/2013/14%20of%202013.pdf

Press Information Bureau, Government of India, Ministry of Defence, 'Initiatives to Strengthen Coastal Security'. 25 November 2014. (Accessed on 12 September 2024.) https://pib.gov.in/newsite/PrintRelease.aspx?relid=111871

The Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices. United Nations Security Council Counter-Terrorism Committee 2018. (Accessed on 10 March 2021.) https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf

United Nations, Development Programme. Sustainable Energy for All. (Accessed on 12 September 2024.) https://www.undp.org/sustainable-energy-all

United Nations, Security Council Calls on Member States to Address Threats against Critical Infrastructure, Unanimously Adopting Resolution 2341 (2017) 2017. Meetings Coverage and Press Releases. (Accessed on 15 February 2021.) https://www.un.org/press/en/2017/sc12714.doc.htm

Unnithan, S. 2001. Ports, Oil Refineries on Gujarat Coast Force New Worries on Overstretched Navy. *India Today.* (Accessed on 25 February 2021.) https://www.indiatoday.in/magazine/defence/story/20010108-ports-oil-refineries-on-gujarat-coast-force-new-worries-on-overstretched-navy-776028-2001-01-08

United Nations Convention on the Law of the Sea (UNCLOS), [2082] Updated, October 2024. United Nations. (Accessed on 15 February 2021.) https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

Vice Admiral Pradeep Chauhan, Physical Protection of India's Critical Maritime Infrastructure: Part 2: Maritime Energy Sector. National Maritime Foundation. (Accessed on 28 February 2021.) https://maritimeindia.org/physical-protection-of-indias-critical-maritime-infrastructure-part-2-maritime-energy-sector/

Vice Admiral Abhay Raghunath Karve, 29 November 2018. Maritime Security: a decade after 26/11. Gateway House. (Accessed on 15 February 2021.) https://www.gatewayhouse.in/maritime-security-after-2611/

Vice Admiral M.P. Muralidharan, 16 January 2021. Indo-Pacific: An Emerging Outlook for the 21st Century. *Indian Defence Review*. (Accessed on 15 February 2021.) http://www.indiandefencereview.com/news/indo-pacific-an-emerging-outlook-for-the-21st-century/

Williams, S.O., 21 May 2014. Offshore Installations: Practical Security and Legal Considerations. Center for International Maritime Security (Accessed on 15 February 2021.) https://cimsec.org/offshore-installations-practical-security-legal-considerations/

Ms. Gargi Sharma
PhD Student
Delhi
India

# Chapter 16: From Global to National Views: Examining Intelligence Gathering as an Intelligence-curbing Policy: A Review Essay

**Adebimpe Saheed Fagbemi**
**ORCID iD: https://orcid.org/0009-0007-1412-3588**

**Nirmala Devi Gopal**
**ORCID iD: https://orcid.org/0000-0002-4060-455X**

## Abstract

It is pertinent to note that insurgency has been a menace to the development of human capital and natural resources on a global scale. No doubt, every state is proffering solutions to curb the threat of insurgent and terrorist groups. This paper will focus on insurgency from the global, regional and national perspectives, adopting three selected countries such as Great Britain, Sri Lanka and France (globe), Kenya (Regional) and Nigeria (National). In addition, timely and accurate intelligence has been used by governments and security agencies to submerge the activities of the insurgent group, yet the war against them still persists. Entrancing intuitions from the prevailing literature, the paper views that the root causes of insurgency need to be addressed timely in order to curtail it. More so, some of the security agencies lacks the modern tools in gathering intelligence such as measurement and signature intelligence (SIGMINT), signal intelligence (SIGINT), geospatial intelligence (GEOINT) and so on. It con-cludes that insurgents group operate differently base on ideology, religion, political motivation, uneven distribution of resources, secession and so on. Nevertheless, with accurate, timely and prompt intelligence sharing the govern-ments and security agencies will able to combat and win the war against terrorists cum insurgents' group.

AASBS Volume #21 (2025) https://doi.org/10.29086/978-0-9869938-0-0/2025/AASBS21
Chapter DOI: https://doi.org/10.29086/978-0-9869938-0-0/2025/AASBS21/16 pp. 365 - 380

**Keywords:** Counterinsurgency, Ideology, Intelligence gathering, Insurgent's group, Security forces.

## Introduction

Insurgency has been a massive hindrance to Nigeria's peaceful coexistence. Terrorism cum insurgency are two sides of the same coin; insurgents utilize terror attacks to perpetrate their nefarious activities such as bombing, killing, kidnapping, robbery and so on (Adegoke 2017). The Nigerian Government has been battling terrorism and insurgency threats for over a decade and has been unable to win the battle due to the lack of strategic and coordinated intelligence (Agbiboa 2018). However, several factors have contributed to the failure to combat and defeat the terrorist group. These, among others, include a lack of timely and reliable intelligence concerning the terrorists, inadequate Intelligence sharing amongst the security agencies, a lack of political will on the part of the government, and failure to address the root causes (Onuoha 2018). Pertinent to note is the point that insurgency poses primary threats to national security and must be treated with vigour by the government (Agbiboa 2017).

## The British Approach in Curbing Insurgency

It is crucial to note the British approached in the war against insurgency. The British experience in Northern Ireland, especially the combat against the Provisional Irish Republican Army (PIRA) that started in year 1969 and they used timely and accurate intelligence to curb the menace of insurgency. Another insurgent group surfaced, and they were active in the Northern Ireland at that period, but PIRA's remained the major threat. The PIRA has been qualified as highly developed in terms of intelligence-led terrorist group because of its functional and capacity precision (Isyaku 2017).

Related to different countries engaging insurgent warfare, the United Kingdom came to the animosity in Northern Ireland with important experience in counter insurgency (COIN) and its current appendage, counterterrorism (Umejesi 2016). Some of the United Kingdom's former insurgent warfare has been held up as examples of efficiency in such wars. Inadequate and inaccurate intelligence gathering were a key origin of the problems. It was reported by historian Chris Ryder that, 'the principal weakness, according to the Chief of

the General Staff who visited the Northern Ireland in 1971was an inadequate intelligence gathering' (Isyaku 2017).

In the bid to curtail insurgency, intelligence must deliver the critical insight needed to understand what actions will be useful and what levels of dedication are required, the tactical insight to attack the insurgent group when military action is used, this operation need to be discreet and properly planned to achieved huge success (Sumner 2004). Different agencies were involved in the intelligence combat against PIRA. From the onset the Royal Ulster Constabulary (RUC), which was expected to lead the intelligence collection to avert insurgency, was not availed to do the needful at the right time (Lowenthal 2002). This made the British Army to interfere in Northern Ireland and impetus it (and other intelligence agencies) to take the lead in intelligence gathering (Casey 2007). As the uprising became more acute, many different intelligence units from the law enforcement, military and intelligence agents were established. More so, national agencies like MI5, MI6, the Secret Intelligence Service and Security Service respectively birthed to gathered political and economy intelligence (Lowenthal 2002).

It is important to note the insurgency in Sri Lanka and how their government won the insurgents war through accurate and timely intelligence. Sri Lanka experiences the deadliest, threat to its sovereignty and stability to the nation since her independence in 1948 from the British government (Wannesburg 2005). The insurgent's war started from late 1970s between the Tamils and the Sri Lankan government. There are two major tribes in Sri Lanka they are Sinhalese and Tamils. The Sinhalese are the majority, consisting of 85% of the population while the Tamils are just 15% (Casey 2007).

According to Tarlebbea (2010) the Tamils tribe later formed an insurgency group called Tamil National Alliance (TNA) which later metamorphosed to Liberation Tigers of Tamils Eelam (LTTE) in 1976, headed by Velupillai Prabhakaran. They engaged in insurgency activities with the Sri Lankan government from 1983 to 2009 in the last stage of the warfare. The LTTE ideology is not religious unlike other insurgents' groups like Boko Haram, ISWAP, ISIS, and so on but separation, secession (Establishment of Tamil Nationalism) and revolutionary socialism. The LTTE insurgent group was one of the deadliest and long insurgencies wars against government. It lasted for about 26 years before the Sri Lanka government were able to crush them through timely intelligence and addressing the root causes. Ethnic rivalry is the major causes of the conflict. The Sri Lankan Tamils consider that they are been marginalized by the government in power, they are victims of economic

and political discrimination in their own nation. The Tamils claim that, since the late 1950s the Sinhalese have dominated the government and have denied them to free access to Sri Lanka's universities and other higher institutions, they equally stopped funding to develop the Tamils areas, they banned the use of Tamil language and declared Sinhalese as the country's official language. All these are the root causes of the insurgency in Sri Lanka (Sumner 2004).

The Sri Lanka government was able to win the war against the deadliest insurgent's group after 26 years. The administration of Lt. Col. Nandasena Gotabaya RAJAPAKSA failed woefully to end the insurgency in the country because he neglected timely intelligence and grand strategy. He focused mainly on military hard power to conquer the insurgents war. Contrary to this, his successor Mahinda RAJAPAKSA the President between 2005 and 2015, adopted grand strategy and intelligence gathering to curtail the LTTE nefarious activities. He used strategic objective that matched the LTTE's principal weaknesses. The grand strategy includes peace sought, economics, military actions, information operations strategy to guide lower-level activities and timely intelligence (Wannesburg 2005).

It is imperative to consider the insurgency cum terrorism in France because they have long time experience and their government was able to curtail it after a long battle through adequate and timely intelligence gathering (Bodunde *et al.* 2019). According to the 2018 Global Terrorism Index, France was ranked 30th in the year 2018 as against 23rd position in year 2017 Global Terrorism Index (Institute for Economics and Peace 2018). Insurgency cum terrorism in France was traced back to the French Revolution (1789-1799) which was referred to as state sponsored terrorism (Akinola and Tella 2013). Also, from the mid-1970s, France and other European nations have witnessed various threats of insurgency and terrorism attacks. In 1985, General Rene Audran of the French Ministry of Defence was assassinated by Guerrilla group action (Thomson 2012).

Terrorist violence in France reduced after state-sponsored terrorist groups from the Middle East beset French interests in the setting of East-West tensions caused by the Cold war. Various insurgents' groups like the Palestinian Abu Nidal Organization (ANO), Lebanese Hizballah, the Jackal were the most active from 1982 to 1987 (Olofinbiyi & Steyn 2018). In 1988, the ANO executed four French nationals on a Greek tourist boat in the city of Porous Hizballah led a campaign of 13 terrorist attacks starting in year1985 that capped with an attack against the store 'Tati' at Rue de Rennes in Paris, killing seven people and about 66 wounded (Oghi 2014).

Akinola (2017) opined that the causes of insurgency and terrorism attacks in France were caused by ideology and regional identity, violence caused by resistance by former French colonies against their persistent domination by France and the current trends of terrorism which is global and inclined to Islam. However, the French government was able to curtail the insurgency menace through intelligence gathering and new counter-terrorism measures like house arrest replaced by surveillance of individuals, establishing cordons around key and vulnerable areas, patrolling and stations of military personnel around places of worship, police raids et cetera. The French government also strengthens the intelligence agencies and provided them with necessary supports to combat the terrorist's activities (Phenson *et al.* 2016).
More importantly, the intelligence agencies in France, have assisted the government to combat the nefarious activities of different terrorist group in the French soil. They are Directorate-General for External Security (DGSE), General Directorate for Internal Security (DGSI), Directorate of Military Intelligence (DRM), Intelligence Processing and Action Against Clandestine Financial Circuits (TRACFIN), Intelligence and Electronic Warfare Brigade (BRGE), National Commission for the Control of Security Interceptions (CNCTR) among others (Sumner 2004).

The French presidency under the leadership of Emmanuel MACRON adopted some strategies to counter terrorism attacks in the country. The French intelligence agents are assigned to keep a close watch and infiltrate the terrorist groups. Intelligence being a major aspect of these approaches. Multiliteralism and training counter- terror operatives were adopted to curb the menace of the insurgency (Mosandi 2019). More so, the use of legal framework empowers the government to deport foreigners that pose a serious threat to public order. The French government has recorded huge success in counter-terrorism efforts using both soft and hard power approaches (United States Department of State 2018).

According to Achumba *et al.* (2016) France has really scored high points in terms of combating terrorism in its shore and fighting terrorism outside its borders. As a global power and the worth the nation places on its citizens explicate the wide gap that occur between its determinations considering this and those of Sub-Saharan countries without such gigantic strides to curb the insurgency vices. In France, the government also introduced Civic Education as parts of school curriculum and school attendance is compulsory up till age of 16. The subject aids the youngsters to understand the implication of insurgency and to deter them from being part of the criminal group as contrary to the Nigerian state where youngsters are brainwashed daily to take part in the Boko

Haram menace. The French government also engaged the Muslims clerics who are anti-jihadist, to support the anti-terrorism efforts and counter foreign radical jihadist propaganda (Mosandi 2019).

Insurgency from the regional perspectives observe painstakingly how government respond to nefarious activities of the terrorists and the counter measures adopted. It is pertinent to note that the insurgency and terrorism menace in Kenya is a reference point to this study. According to Global Terrorism Index, Kenya was ranked 22nd in the year 2017 but ranked 19th position in the year 2018 (Institute of Economics and Peace 2018). This implies that insurgency cum terrorism activities in the state has worsened and need to be curtailed. There are numerous root causes of terrorism in Kenya, where few will be explained. The state of Kenya suffers more than its shares in terms of counter terrorism approach (Mosandi 2019). Bodunde *et al.* (2019) posits that the porous borders have contributed immensely to the menace of terrorism in Kenya. The country borders with 5 countries which are Tanzania, Uganda, Sudan, Ethiopia and Somalia. Kenya's eastern and northern neighbours' are Ethiopia and Somalia. These borders in the axis are too porous which give room for the Al Shabaab Terrorist group from Somalia to invade and target Kenya without being apprehended by security forces. More so, the slow response of the government in countering insurgency makes the state more vulnerable. Local tensions are another germane root causes of terrorism in the Kenyan state, the Northeast along the coast are mainly inhabited by the Muslims, which make up of a tenth of the Kenya's population. The region is not developed, due to lack of both public and private investments. It leads to tension and some locals in the region are disgruntled and feel cheated and marginalised by the Kenyan government (Agbiboa 2019).

Despite the intelligence agencies and countermeasures adopted by the Kenyan government to curtail the long war against insurgency cum terrorism, the state has failed woefully in combating the menace. The Kenyan state has three intelligence agencies; these are the Special Branch (SB), Directorate of Security Intelligence (DSI) and National Security Intelligence Service (NSIS). The SB and DSI are saddled with the procurement of domestic intelligence on both civil and military affairs while the NSIS is responsible for both gathering of domestic and foreign intelligence. The Kenyan government has responded in both hard and soft approaches to combat the menace of insurgency. The hard approach includes the establishment of an Anti-Terrorism Police unit in 1998 in which some of the troops are deployed to Somalia and Ethiopia borders. The soft approach measures include institutional building policy, bilateral/

multilateral cooperation with the United Kingdom and United States, legislative reform (Faluyi *et al.* 2019).

The Kenyan government has failed to win the battle against the terrorist's group because the intelligence agencies lack gathering of timely and actionable intelligence and they are not financially motivated. Also, the government and the security forces did not gain the full supports of its citizens especially the natives of Mombasa community in the eastern region of the country (Phenson *et al.* 2018).

Observing insurgency menace from the view of National perspective, adopting the Nigerian state as a reference point. The Nigerian state attained her nationhood in 1914 but got her independence 1960 from the Great Britain. The nation has experienced various social vices such as religious sect, political violence, communal clashes, land disputes, kidnapping, arson, and so on (Mosandi 2019). The history of terrorism and insurgency could be traced to religious intolerance and violence during those early eras was now ill-famed Maitasine sect. The group was established by Muhammed Marwa, a radical Islamists in the Northern region of the country. The Maitasine sect had an ideology that contradicted to the social norms and the real teachings of Islamic religion. Their members were mostly illiterate, jobless youths, unwary and low self-esteemed. They are sponsored by Saudi Arabia Wahabi/Salafi sect of Islam, both financially and in teachings (Olofinbiyi & Steyn 2019).

The Wahabi/Salafi sect of Islam has been adopted by the Maitasine group. They were intolerant and extremist in the course of practising their religion. They were disposed to violence at the slightest incitements. The aggressive and intolerance led to the riot in Kano between them and the Kano Government in 1980. The riot was regarded as the worst religious conflict in Nigeria until the emergence of Boko Haram Group (BHG) in 2009. Although, the Boko Haram group was founded in 2002 has a non-militant group. During the Kano riot by the religion sect, over 40,000 people were killed, 10,000 innocent civilians were internally displaced and property worth of billions of naira (Nigeria currency) were destroyed (Achumba *et al.* 2016).

The leader and creator of the radical sect, Muhammed Marwa was later killed by the Nigerian security Forces and the group was crushed. The Nigerian security forces thought that had won the battle against the deadly religious radical sect in the history of the country and they had crushed the ideology of religious intolerance and extremists. Thereafter, the deadliest insurgent group known as Boko Haram Group surfaced. This insurgent group has been engaging the Nigeria security forces in a guerrilla warfare since 2009 and remains active

11 years later. They have killed more than 32,000 people since 2009 till 2019. Over 3 million people have been displaced internally and outside the shores of the country (Mosandi 2019).

According to the Global Terrorism Index, Nigeria was ranked 3rd position since 2016 till 2020 and the deadliest country in term of terrorism and insurgency attacks in Africa (Institute for Economics and Peace 2020). It is germane to note the root causes of terrorism and insurgency and various factors that led to the emergence of it in the Nigerian state. According to Thomson (2012) the insurgent's group was driven by perceived oppression, religious extremism, poverty, ignorance, ideological orientation, lack of political will and ethnic thoughts. More so, Ukpong-Umo (2016) posits that insurgency occurred in Nigeria due to failure of governance, lack of strong culture that enables citizens to make real demands from their leaders and weak security architecture. He stressed further that the environment in which Nigerians domicile and the involvements of governance are the possible causal factors of the emergency of insurgency.

Sani (2011) cited in Mu'azu (2011: 18-19) maintains that the Boko Haram Group was instigated by various factors which are repressive attack against the religious group leader (Muhammed Yusuf) who was killed by the government security forces all in the name that he wanted to escape from a lawful custody in 2009. The Boko Haram group were excluded in all the activities of mainstream of Islamic groups, failure in governance in all the North East region states, they felt cheated that federal government policy favour is against their ideology. In addition, the proliferation of arms and ammunitions, aftermath of Chadian war which led to illegal migration, no connection between both elected and appointed leaders and the people, lack of data base and intelligence about individuals and organisations that have connections with foreign allies, there is no rehabilitation center for religious fundamentalists, all these are the root causes of terrorism and insurgency which required holistic approach, accurate and timely intelligence to curtail.

The Boko Haram group has inflicted different terrors on the security forces, innocents' civilians and Nigerian government. It is pertinent to discuss these major terrorism and insurgency that occurred between 2009 till date. The first ever bombing in Nigeria shores was carried out by BHG member, Mohammed Manga (35 years) young man, on 16$^{th}$June 2011 that was the first suicide bomber in Nigeria (Mosandi 2019). This man left his home and drove to Abuja on a deadly mission to bomb himself and the Nigeria Police Headquarters. He was a businessman and financially he was stable to some

extent but because of his ideology he volunteered himself to go on the deadly mission as a suicide bomber, all in the name of religion and going to paradise after the terror mission (Akinola & Tella 2017).

## Research Methodology

The use of desktop publishing in research methodology allows for the effective organization, analysis, and presentation of data. By adopting advanced publishing tools, this study aims to provide a comprehensive understanding of how intelligence gathering can function as an intelligence-curbing policy, from a global to a national perspective. To reiterate, this paper is desktop research, which was conducted using the purposive sampling method to select articles from different research engines such as Google Scholar, Science Direct, and EBSCO. These articles were selected based on three criteria, which are, (i) appearing in the first 10 search results; (ii) space - intelligence context; and (iii) most relevant to the purpose of this paper.

## How Intelligence Gathering can Assist in Curbing Terrorism, Insurgency and Other Vices

The intelligence agencies are saddled with the high level of procurement of timely, accurate and adequate information which will be collated, evaluated, analysed and interpreted before becoming intelligence that will be useful for the government in policy and decision making or the security agencies that required it for the safety and wellbeing of the masses (Onuoha 2017).

According to Bodunde *et al.* (2019) opined that intelligence gathering is a procurement of information of value, about a person of security interest, building or structures, activities of hostile intelligence services (HIS) that can be processed through three closely items collection, evaluation and interpretation to form intelligence. The aim of intelligence gathering is to curtail the menace of the enemies of state before perpetrating the evil acts. The Nigerian government is still battling with terrorism cum insurgency of the BHG because the security agencies have not gotten the real intelligence about their sponsors, collaborators, strength, and weakness and so on.

Ashaolu (2017) posits that there are various challenges that inhibit the accurate information that can be processed to timely and useable intelligence. These challenges are lack of intelligence sharing amongst the security agencies.

The security agencies in Nigeria promote lack of cooperation, ego boosting, overbearing and favouritisms. These factors have tremendously affecting the intelligence gathering. More so, sometime the government when they are provided with intelligence, they politicised and make a mockery of intelligence sharing amongst the security agents.

According to Bodunde *et al.* (2019) the Nigerian security are not information sensitive and the consciousness of the security operatives must be improved in terms of training and memory training. Hence, this lapse has affected them in terms of intelligence gathering in a battle against terrorist, insurgent and a mapping strategy to defeat them.

The intelligence community (DSS, DIA and NIA) in their collective ability, remains the eye of protecting various essential blind spots in our society as they relate to the wellbeing and safety of the citizen. To some level, security agencies failed to forestall security lapses in Nigeria, the duty of intelligence agencies is to procure timely and accurate intelligence which must be proactive in nature but not reactive as we witness today in the Nigerian state (Isyaku 2017).

Faluyi *et al.* (2019) posits that effective counterinsurgency, prevention, protection, preparedness, response and revitalization efforts depend on accurate, timely and achievable information about the targets, where and how they operate, their cohorts, and the possible vulnerable entity which the enemies may attacks. Presently, the Nigerian state is confronted with various degree of insecurity such as insurgency, terrorism, bombing, kidnapping, armed banditry, cattle rustling, proliferation of arms and ammunitions, influx of illegal migrants, porous borders, corruption, weak and corrupt judiciary, marginalization, poverty, and so on. The security agencies have a significant role in curtail each of these threats.

Despite the challenges of intelligence gathering and interagency synergy remain the greatest and apt in counter measure against insurgency and other security breaches (Ashaolu 2017). The main challenge in intelligence gathering is intelligence sharing. Most of the intelligence gathered are not shared amongst the security agencies in the state. Intelligence sharing is meant to enable the use of activities, from protecting people from violent threats, locating and apprehending suspects (Onuoha 2017).

Intelligence sharing is the ability to exchange intelligence information data or knowledge amongst federal, state, local and provide sector unit. The intelligence from experts is to be shared and used timely among the security agencies. It is necessary for the entire Nigerian citizen to render useful informa-

tion to the security agents, which will be processed to intelligence and shared by the security agencies (Umejesi 2016).

It is imperative to focus and briefly discuss the levels of intelligence sharing amongst security agents. It is conducted and shared at various levels namely strategic level, tactical level, operational level and counterinsurgency level. Strategy Level Intelligence is the largest among the level of intelligence sharing because it involves national and international agencies. It concerns extensive issues about political, military capabilities, economic, scientific, technology, non-state actors and so on. It entails the issues of international and national that concern security (Ashaolu 2017).

Tactical Level Intelligence assist the intelligence agencies and government in planning and combat readiness. It involves briefing, deployment and current threats on flash and black spots to the patrol team. The patrol team will be examined to elicit valuable information for processing and communicating through appropriate channels. The Operational Level Intelligence is intensive on support, focuses on collecting and analysing information that identifies and locates the real threats. The Counterintelligence Level is the process of sharing timely and processed information to protect, safeguarding and preserve the secret of a state's intelligence by averting espionage activities from infiltrating the nation's government such as intelligence community, military strength, economic and so on (Bodunde *et al.* 2019).

## Conclusion and Recommendations

Basically, terrorism and insurgency are threats to National security in which almost every state are affected directly or indirectly. Critical review of journals and some materials reveals that the aims of insurgent's group are different from one and another. For instant, the Tamils Eelam insurgent's group in Sri Lanka are fighting for secession and uneven distribution of resources, while the Boko Haram Group in Nigeria are ideology, political motivated, bad governance, marginalization. More so, the study identifies the major causes of insurgency in the globe such as nepotism, favouritism ethnocentrism, cultural identity, bad leadership, unemployment, high rate of illiteracy, religious fundamentalism, and so on. If the governments could focus on the grey areas stated above the rate of terrorism cum insurgency will be reduced drastically.

The study also recommends that accurate, timely and sharing of intelligence will be apt to curtail the menace of insurgency in the globe, regional and national. The security agencies especially the intelligence community

should be trained more on intelligence gathering and sharing. It is incumbent on them to be trained on how to use the modern gadgets of intelligence gathering to counter any forms of criminality in the state. The issue of egocentrism amongst the security agencies should be condemned by the government, this will foster security liaison and strengthen their relationships. Accurate, timely and sharing of intelligence will assist the governments and the state to conquest any form of menace against the contemporary threats.

The study identifies that insurgency are experienced in a different way by different insurgent's group. The way to tackle it are diverse but the method is still the same which is 'accurate and timely intelligence gathering'. There are various forms of intelligence gathering ranging from human intelligence, signal intelligence, imagery intelligence, measurement and signature intelligence, open source intelligence and geospatial intelligence. When all these various forms of intelligence are used properly no doubt, the government will win the war against terrorism and insurgency. The security agencies should be well trained on both covert and overt operations, highly motivated both monetary and incentives, this will enhance their loyalty and professionalism in discharging their statutory mandate.

The study recommends the implementation of a community policing method as another realistic paradigm shift towards counter insurgency cum terrorism strategy. This paper submits that the Nigerian government should embrace this method as an alternative way of curtailing the menace of the Boko Haram group should the negotiation approach flop. No doubt, the community policing will play a critical and substantial role in eradicating and curbing the activities of insurgents in terms of gathering accurate and reliable information about them, which will be processed to intelligence. It is factual that, intelligence gathering is key in combating asymmetric or non-asymmetric warfare.

Lastly, this paper recommends that the government and the security agencies should engage the masses in community sensitisation programmes about terrorism cum insurgency and the adverse magnitudes of such events and circulating the information amongst the communities are key, particularly in remote populations prone to attacks. The phase of awareness of the consequence of insurgency should be strengthened amongst the residents. The federal government of Nigeria, through the various ministries and agencies such as Ministry of Information and Culture, National Orientation Agency, National Broadcasting Commission, Voice of Nigeria et cetera, should be used effectually to educate the masses on the havoc and consequences of associating

or connecting with the insurgent group via radio, television, banners, sign posts. This will deter the masses and the effervescent youths from being involved in dread acts.

## References

Achumba, I.C., O.S. Ighomereho & M.O.M Akpan-Robaro 2016. Security Challenges in Nigeria and the Implications for Business Activities and Sustainable Development. *Journal of Economics and Sustainable Development* 4,2: 79 - 99. https://doi.org/10.9774/GLEAF.8757.2016.ju.00007

Adegoke, N. 2014. *Research Methods in Social Sciences.* Lagos, Nigeria: Prime Targets Limited.

Adegoke, N. 2017. Intelligence Gathering and Challenges of Insecurity in Nigeria. *Journal* 3,2: 4-12.

Agbiboa, D.E. 2018. Ethno-Religious Conflicts and the Elusive Quest for National Identity in Nigeria. *Journal of Black Studies* 44,1: 3 - 30. https://doi.org/10.1177/0021934712463147

Agbiboa, D.E. 2019. National Heroes or Coming Anarchy? Vigilant Youth and the 'War on Terror'. *Nigeria Critical Studies on Terrorism* 11,2: 272 - 290. https://doi.org/10.1080/17539153.2017.1400497

Akinbi, J. 2015. Examining Boko Haram Insurgency in Northern Nigeria and the Quest for permanent Resolution of the Crisis. *Global Journal for Arts, Humanities and Social Sciences* 3,8: 30 - 42.

Akinola, A. & O. Tella 2017. Boko Haram Terrorism and Nigeria's Security Dilemma: Rethinking the State's Capacity. *International Journal of Innovation Science and Humanities Research* 1,3: 70 – 78. https://www.researchgate.net/publication/260201390_BOKO_HARAM_TERRORISM_AND_NIGERIA'S_SECURITY_DILEMMA_RETHINKING_THE_STATE'S_CAPACITY

Ashaolu, A. & O. David 2017. Solving Security Challenges in Nigeria through Intelligence Gathering and Surveillance. *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2275986

Azumah, J. 2015. Boko Haram in Retrospect. *Islam and Christian Relations* 26,1: 24 - 43. https://doi.org/10.1080/09596410.2014.967930

Bodunde, J., N. Balogun & G. Layefa 2019. Intelligence Sharing; The

Challenges among the Nigerian Security Agencies and Government. *Global Scientific Journal* 7,6: 36 – 47.

Buchanan-Clarke, S. & R. Lekalake 2016. Extremism in Africa: Public Opinion from the Sahel, Lake Chad and the Horn of Africa. Afro Barometer Policy Paper No 32.

Burgess, R.L. & R.A. Akers [1966] 2014. A Differential Association-Reinforcement Theory of Criminal Behaviour. *Social Problems* 14,2: 128 - 141. https://doi.org/10.2307/798612 https://doi.org/10.1525/sp.1966.14.2.03a00020

Casey, J. & M. Mitchell 2007. Requirements of Police Managers and Leaders from Sergeant to Commissioner. *Police Leadership and Management Journal* 4 - 20. Federation Press. https://www.researchgate.net/publication/347463928_Police_Leadership_and_Management

Creswell, J.W. 2015. Integrating Quantitative and Qualitative Results in Health Science Mixed Methods Research through Joint Displays. *The Annals of Family Medicine* 13,6: 554 - 561. https://doi.org/10.1370/afm.1865 PMid:26553895 PMCid:PMC4639381

Faluyi, O.T., S. Khan & O.A. Akinola 2019. Boko Haram's Terrorism and the Nigerian State Federalism, Politics and Policies. Cham, Switzerland: Springer.

Institute for Economics and Peace 2018. Global Terrorism Index. Measuring and Understanding the Impact of Terrorism. https://reliefweb.int/report/world/global-terrorism-index-2018

Isyaku, A. 2017. Terrorism: A New Challenge to Nigerian Stability in the 21st Century. *International Affairs and Global Strategy* 14, 2: 21 - 34.

Lownethal, M.M. 2002. Intelligence: From Secrets to Policy. 2nd Edition. Washington D.C: Congressional Quarterly Press.

Mosindi, C. 2019. Global War on Terror: The Nigerian Dimension - Kindle edition. Pp 178 - 245.

Mu'azu, A. 2014. The Rise of Boko Haram, a Radical Islamist Sect. *The Journal of Peace Research* 40,5: 507.

Murray. Y. 2000. *Police and the Challenges of the 21st Century: Managing Change in Police Organisations.* Ontario: Canadian Police College.

Ngboawaji, O.N. 2017. An Analysis of Intelligence Support to Security Operations in Nigeria: A Review of Some Joint Task Force Operations. *Peace and Security Review* 5,9, First Quarter: 1 - 23. Retrieved Online.

Oghi, F.E. & J.O. Nnumen 2014. Military Intelligence and the Challenge of National Security in Contemporary Nigeria. *International Journal of Research in Humanities and Social Sciences* 1, 2.

Olofinbiyi, S.A. & J. Steyn 2018. The Boko Haram Terrorism: Causes Still Misunderstood. *Journal of Social Sciences* 14: 129 – 144. https://doi.org/10.3844/jssp.2018.129.144

Olofinbiyi, S.A. & J. Steyn 2019. The Boko Haram Impasse: Community Policing as a Nostrum for Conflict Resolution. *Journal of Homeland Security and Emergencies Management.* https://doi.org/10.1515/jhsem-2019-0011

Onuoha, F.C. 2014. The Islamist Challenge: Nigeria's Boko Haram Crisis Explained. *African Security Review* 19,2: 50 - 62. https://doi.org/10.1080/10246029.2010.503061

Onuoha, F.C. 2018. Boko Haram and the Evolving Salafi Jihadist Threat in Nigeria. In Monocles, M. (ed.): *Boko Haram: Islamism, Politics, Security and the State of Nigeria.* Leiden: African Studies Centre.

Osumah, O. 2017. Boko Haram Insurgency in Northern Nigeria and the Vicious Cycle of Internal Insecurity. *Small Wars and Insurgency* 24,3: 536 - 560. https://doi.org/10.1080/09592318.2013.802605

Phenson, U.A., P.A. Ojie, J.O. Esin & A.J. Atai 2018. Essential Elements of Security and their Applications in Ensuring Stability and Integration of Nigeria. *International Journal of Politics and Good Governance* 5,5:3.

Sanni, D. 2011. Boko Haram Attacks Adamawa Village, Raze Hospital, Houses. (Accessed on 1st December 2014.)

Sumner, B.T. 2004. Territorial Disputes at the International Court of Justice, *Duke Law Journal* 53: 1779.

Tarlebbea, N.K. *et al.* 2010. The Cameroon and Nigeria Negotiation Process over the Contested Oil Rich Bakassi Peninsula. *Journal of Alternative Perspectives in the Social Science* 2,1: 198 - 210.

Thomson, V. 2012. Boko Haram and Islamic Fundamentalism in Nigeria, *Global Security Studies* 3,3.

Tobin, D.L., K.A. Holroyd, R.V. Reynolds & J.K. Wigal 1989. The Hierarchical Factor Structure of the Coping Strategies Inventory. *Cognitive Therapy and Research* 13,4: 343 - 361. https://doi.org/10.1007/BF01173478

Totten, M.J. 2014. The Rise of Boko Haram. *World Affairs Journal.*

Ukpong-Umo, R.E. 2016. Insurgency in Nigeria and the Challenge of Nationhood. *Nigerian Journal of Rural Sociology* 16: 64 - 69.

Umejesi, I. 2016. The Nation State, Resource Conflict, and the Challenges of 'Former Sovereignties' in Nigeria. *African Studies Quarterly* 13,3.

United State Department of State. The Office of Electronic Information, Bureau of Public Affairs. (Accessed on 26 November 2018.)

Waldek, L. & S. Jayaseka 2017. Boko Haram: The Evolution of Islamist Extremism in Nigeria. *Journal of Policing, Intelligence and Terrorism* 6,2. https://doi.org/10.1080/18335330.2011.605217

Wannesburg, G. 2005. Organized Crime in West Africa. *African Security Review* 14,4. https://doi.org/10.1080/10246029.2005.9627583

Adebimpe Saheed Fagbemi
Department of Criminology & Forensic Studies
Howard College
University of KwaZulu-Natal
Durban

Professor Nirmala Devi Gopal
Department of Criminology & Forensic Studies
Howard College Campus
University of KwaZulu-Natal
Durban, South Africa
Gopal@ukzn.ac.za

# Chapter 17: Psychological Security – Exploring Community Engagement in Peacekeeping

**Matshepo Matoane**
**ORCID iD: https://orcid.org/0000-0002-1824-384X**

## Abstract

Psychological security is intertwined with peacekeeping, based on the feeling of security. Community engagement is a practice that is employed in peacekeeping to ensure security of communities. Adopting a qualitative case study approach and community psychology as a conceptual framework, this chapter seeks to understand how community engagement ensures psychological security of communities. The chapter argues that psychological security within peacekeeping is dependent upon the conscious and active participation of communities for which security is required. The chapter further argues that representations of community and positions adopted in understanding this concept, have a bearing on how communities are engaged with. The study revealed that a subjective representation of community is associated with community empowerment, while an objective or value free representation of community is associated with a partially empowered community. Communities who feel empowered may be more likely to perceive psychological security in their environment.

**Keywords**: peacekeeping, psychological security, community engagement, community psychology

# 1 Introduction

The concept of security, in the field of psychology, dates back to the time of Abraham Maslow, who identified security as one of the foundational basic human needs contributing to psychological wellbeing. Later, Maslow and other scholars coined psychological security (Bar-Tal & Jacobsen 1998; Cummings & Miller-Graff 2015; Jia, Li, Li, Zhou, Maslow 1942; Wang, Sun & Zhao 2018; Zotova & Karapetyan 2018), a term that denotes feelings of safety and belongingness; having a sense of control over the social environment and feelings of confidence in freedom from fear (Maslow 1942).

Bar-Tal and Jacobsen (1998) in their application of psychological security within peacekeeping, submit that a feeling of security is dependent on a person's perspective, thus this renders security a subjective concept. According to these authors, individuals first perceive the external environment/event, evaluate them (based on a repertoire of their beliefs) and subsequently determine their feelings of security. It is for this reason that Bar-Tal and Jacobsen (1998) argue that in addition to understanding security in political, societal and economic terms, we also need to understand it from a psychological perspective. Similarly, this chapter focusses on psychological security within peacekeeping. Acknowledging the varied roles of psychologists and peacekeeping forces, I adopt Maslow's definition of psychological security to refer to communities' sense of control over their environment, including their feelings of confidence from fear. As fundamental principles, it is my view that:

1. Psychological security is not something that can be offered to people, it is dependent on conscious and active engagement [on the part of the individual/group/community under consideration]

2. Psychological security within peacekeeping is dependent upon conscious and active participation of communities for which security is required.

I am therefore interested in understanding the practices that are currently being used in peacekeeping to ensure the security of communities. Community engagement is one such practice, hence its central focus in this article.

The United Nations (UN) is widely known for providing human security through peacekeeping missions. The UN Multi-dimensional Integrated

Stabilization Mission in the Central African Republic (MINUSCA), the UN Multidimensional Integrated Stabilization in Mali (MINUSMA), the UN Organization Stabilization Mission in the Democratic Republic of Congo (MSONUSCO), and the UN Mission in South Sudan (UNMISS) constitute some of the largest multi-dimensional peacekeeping operations (Henigson 2020). Peacekeeping is a vehicle for providing communities with a sense of safety and freedom from fear as articulated in its mission of controlling and resolving armed conflict (Goulding 1993) and protecting civilians from physical violence (Gorur & Carstensen 2016). In response to the divergent views on the effectiveness of UN peacekeeping operations, Hultman, Kathman, and Shannon (2013) argue that the size and capabilities of peacekeeping missions, as well as the mandate of UN personnel, play a significant role in determining the success or failure of these missions.

There have been several notable developments in peacekeeping – peacekeeping missions changed from simple observable missions to multi-dimensional and multidisciplinary approaches, ultimately leading to a focus on the protection of civilians (POC) (Singh 2020). Additionally, shifts from negative conceptions of peace to positive conceptions of peace; the object of peace shifted from the global to the national and ultimately the local context (Gizelis, Dorussen & Petrova 2016). Gizelis *et al.* (2016: 2) submit: 'whereas originally peacekeeping was aimed to secure the objectives of major powers and national elites, its main focus now firmly includes civilians caught up in the fighting and suffering the consequences of poorly governed or failed states'. These are aligned with shifts towards more people-centered approaches to peacekeeping and community engagement (Henigson 2020; Rupesinghe 2016), which were promulgated at the recommendation of the High-level Independent Panel on Peace Operations (HIPPO) report, the Advisory Group of Experts (AGE) for the Review of the UN Peacebuilding Architecture, the Global Study on the Implementation of Resolution 1325 on Women, Peace, and Security, as well as the 2030 Agenda for Sustainable Development (Rupesinghe 2016). Gordon and Young (2019), Krishnan (2020), and Julian and Schweitzer (2015) refer to *community cooperation*, the *responsibility to protect* (R2P), and *unarmed civilian peacekeeping* (UCP) respectively, as additional reforms to peacekeeping, concepts which relate closely to community engagement. These reforms were largely motivated by growing criticisms against peacekeeping practices that were largely state-centric and applied a 'one-size-fits-all' approach to diverse contexts, with a limited focus on political solutions (Henigson 2020; Rupesinghe 2016). Key features of these reforms entail

people-centric and bottom-up approaches geared towards being responsive to community needs and local people (Henigson 2020; Rupesinghe 2016).

Approaches to peacekeeping that are people-centred, bottom-up and responsive to community needs resonate with the notion of conscious community participation and active engagement in the achievement of psychological security. These shifts towards community engagement in peacekeeping led to interest in the current study. This study seeks to understand:

1. The community *as* beneficiary in peacekeeping;

2. The practice of community engagement in peacekeeping; and

3. The attainment of psychological security in community engagement.

## 2 Methodology

This study adopted a qualitative case study approach to understanding community engagement as a vehicle for attaining psychological security in peacekeeping. Gerring (2004) argues that case studies tend to be more useful when they are descriptive, exploratory and they favour propositional depth over breadth and boundedness. Thus, this study provides an in-depth descriptive analysis of how community engagement is applied in peacekeeping to achieve psychological security. This study is therefore bounded within the confines of community engagement and peacekeeping.

The primary source of data for this study was the *Practice Note*, a document that was developed by the United Nations (UN) Department of Peacekeeping Operations-Department of Field Studies (DPKO/DFS) (2018). This is a key strategic document for understanding the policies and practical approaches in fragile and conflict-affected settings. Additionally, Community Psychology is used as a conceptual framework for the study. According to Baxter and Jack (2008: 553) a conceptual framework 'provides a researcher with the opportunity to gather general constructs into intellectual *bins*…and serves as an anchor for the study'.

## 3 Conceptual Framework

In this paper, community psychology is used as a framework for exploring community engagement in peacekeeping. Community psychology as a sub-

field of and approach to psychology has its roots in the Americas, Europe, Asia, Australia, and New Zealand and emerged as such during the 1960s and 1970s (Ngonyama ka Sigogo, Hooper, Long, Lykes, Wilson & Zietkiewicz 2004; Yen 2007). Seedat and Lazarus (2011; 2014) argue that while some manifestations of community psychology in South Africa may have been noted as early as the 1930s, community psychology [as we know it today] only emerged in the mid-1980s. This [present-day] community psychology, they posit, was birthed from psychology's struggles against apartheid racism and socioeconomic exploittation. Some of the justifications for rethinking the place of mainstream psychology in the South African context include questioning the relevance of Western/ European psychological theory within the South African context, including the relevance of clinical and counseling psychology modalities which mostly privilege a few, elite individuals in South Africa (Berger & Lazarus 1987; Dawes 1985; Seedat, Cloete & Shochet 1988; Yen 2007).

Scholars agree that community psychology is an evolving sub-discipline/approach (Ngonyama ka Sigogo *et al.* 2007; Naidoo 2000; Seedat & Lazarus 2011) This affects the manner in which the concept is defined. Naidoo (2000) presents Lewis *et al.*'s definition as follows: 'community psychology refers to a comprehensive helping framework of intervention strategies and services that promote the personal development and well-being of all individuals and communities' (p. 8). This definition places emphasis on community psychology as an approach. At the same time, Naidoo (2000) acknowledges the sub-discipline nature of community psychology, when he underscores the role of cultural norms and traditions and collaboration in the development of community intervention programs. I want to also present a definition of community psychology by Seedat, Duncan, and Lazarus (cited in Yen 2007: 383): - community psychology is concerned with:

- extending mental health services to all citizens, in particular, the historically unserved, underserved, and oppressed;
- transforming the way in which the genesis and development of psychosocial problems are conceptualized and understood;
- providing a contextual analysis that takes cognizance of social issues and addresses environmental stressors;
- radicalizing the praxis of psychological service delivery to include prevention initiatives; and

- redefining the role of psychologists towards a broader public health portfolio that embraces the functions of advocacy, lobbying, community mobilization community networking, and policy formulation.

Seedat *et al.*'s definition, while expanding on Lewis *et al.*'s definition, adopts a radical, transformative stance. The above definition provides an understanding of community psychology as concerned with addressing the structural and systemic challenges impacting individuals, groups, and whole communities. Naidoo (2000) agrees that an understanding of behaviour requires focusing on both an intra-psychic and a systems perspective. I, therefore, premise this article on the understanding that community psychology is aimed at facilitating change and transforming communities.

Acknowledging the developmental nature of community psychology, Seedat and Lazarus (2011) call for the sub-discipline/approach to consider rethinking and re-theorizing its notions of community, social change, and transformation in order to meaningfully engage socio-political developments. It stands to reason, from this call, that as socio-political and ecological environments evolve, new issues emerge, which would require focused attention. I, however, believe defining a broad strategic focus/ideology [similar to the one already defined for community psychology] sets the trajectory for the sub-discipline/approach and will adapt to changing/prevailing community needs.

In concluding this section, I would like to focus on some of the principles and models of community psychology.

Key principles of community psychology include collaboration, participation, empowerment, action and change, and social justice (Carolissen *et al*. 2010; Naidoo 2000; Perkins & Zimmerman 1997; Rappaport 1981; Yen 2007). Interventions in community psychology place greater emphasis on collaboration between communities and psychologists. The first thing that community psychologists do when they enter a community is to conduct a needs assessment, an aspect of which entails identifying key members of the community who should be consulted. The other aspect entails letting communities identify and communicate their own needs, and together, design interventions. This is a critical process for community psychologists as they believe communities are collaborators and they should actively take charge of their own processes for change and transformation to happen within communities. Equally, the emphasis is on bottom-up approaches – communities are regarded as experts on their own issues and are thus better placed to influence the direction of community interventions. Rappaport (1981) explains empower-

ment from a binary perspective, viz. wellness vs illness; competence vs deficits, and strengths vs weaknesses, thus advocating for a positive approach to community mental health. Perkins and Zimmerman (1997) are of the view that for communities to be empowered, they need to be given the opportunity to develop their knowledge and skill, through engaging as collaborators with community psychologists, instead of engaging with them as authoritative experts.

Community psychology adopts four models to intervene in communities, these are – mental health model, the social action model, the ecological model, and the organizational model (Butchart & Seedat 1990; Ngonyama ka Sigogo *et al.* 2007). The mental health model emphasizes the prevention of mental health problems of those living in a particular catchment area and regards mental health as the absence of mental illness (Butchart & Seedat 1990). Critiques of this model see the model as locating mental health problems within communities, with little or no consideration for wider, socio-economic complexities (Butchart & Seedat 1990; Ngonyama ka Sigogo *et al*. 2007). The ecological and organizational models are primarily concerned with group processes and change. The organizational model operates under the assumption that communities are not able to manage themselves and have thus often been accused of being too focused on managing people, contexts, and processes (Ngonyama ka Sigogo *et al.* 2007). This has a bearing on their ability to perceive communities as collaborators. On the other hand, the ecological model seeks to understand the impact of the interaction between people, their environment and their mental health. It is for this reason that some of the critiques of this model argue that implementing interventions, within this model, is hampered by the complexity of the environment (Ngonyama ka Sigogo *et al.* 2007) All three models are said to focus on ameliorating mental health issues as opposed to effecting transformation (Butchart & Seedat 1990; Ngonyama ka Sigogo *et al.* 2007). Butchart and Seedat (1990) discuss the social action model, which understands psychological problems as a product of inequalities that emanate from economic exploitation and political powerlessness. Communities are thus mobilized to take collective action as a way of addressing these structural issues.

The foregoing discussions have projected community psychology as an evolving sub-discipline/approach, which seeks to change the conditions of whole communities by focusing on structural and systemic issues. The principles of community psychology seek to engage communities in participating actively in changing their conditions and in certain instances, transforming their environment and lives. Thus, aiming at instilling a sense of control, by the community, over their environment (psychological security). I do acknowledge,

though that not all models used in community psychology allow for radical transformation, as per the liberatory stance of the sub-discipline/approach.

The key tenants of community psychology, as discussed in this section, provide a conceptual framework for exploring the concept of community engagement in peacekeeping as detailed in the sections that follow.

## *3.1 Community as Beneficiary in Peacekeeping*

Under this section, I seek to explore how the concept 'community' has been used and is understood in community engagement, alongside the use of the concept in community psychology. I argue that the representations of 'community' and positions adopted in understanding the concept have a bearing on how communities are engaged with, i.e. is the engagement empowering or disempowering the community?

Butchart and Seedat (1990) conducted an extensive analysis of the concept 'community', from a Community Psychology perspective. These authors argue that it is difficult to understand this concept outside of the South African political landscape. They thus discuss the concept in relation to *domination* and *liberation* discourses as well as within the *discipline of psychology*. They argue that the South African government [during apartheid] used the concept as a deliberate act to maintain their oppression over the oppressed. A distinction is made between 'imagined' communities and the use of 'community' as a euphemism for race and/or ethnicity. According to Butchart and Seedat (1990) the apartheid government 'imagined' communities to preserve the rights and interests of the minority oppressors. At the same time, the term 'community' carries positive connotations, hence its use as a euphemism for race and ethnicity. Prevailing views exist on community psychology as a psychology of black issues, reserved primarily for black psychologists, with little relevance to white psychologists (Ngonyama ka Sigogo & Modipa 2004). Strengthening these views, Carolissen *et al.* (2010) illustrate how apartheid legislative frameworks impact perceptions of 'community' as meaning black, middle- and working-class individuals.

The above notions of 'community' seem to resonate with how this concept was used in the South African liberation discourse (Butchart & Seedat 1990). Thornton and Ramphele (in Butchart & Seedat 1990) are of the view that liberation movements used the concept to refer to wider sociopolitical groups [like the black community…in townships] operating under the assumption of the existence of a community of 'purpose', represented by people [the com-

munity] who act for a common goal. The above representations of community introduce us to 'community' as [also] denoting geographical locations.

Understanding 'community' within the field of psychology shifts the focus from the individual to whole groups, organizations, and communities, including the role and impact of social systems (Butchart & Seedat 1990; Carolissen *et al.* 2010). In their critical analysis of the mental health and social action models of community psychology, Butchart and Seedat (1990) observe that from the perspective of the mental health model, 'community' is defined in terms of geographical boundaries. On the other hand, community, from the perspective of the social action model is defined both in terms of geographical and socio-political boundaries. According to Butchart and Seedat (1990), these representations imply that community is a socially constructed concept.

Looking at the representation of 'community', from the community engagement perspective, I found the concept to be defined from two main vantage points – the territorial or geographic and the relational, as per Gusfield's definitions (cited in Obst, Zinkiewics & Smith 2002). Territorial/geographic community refers to a sense of belonging to a particular area, which could be a neighborhood, town, city, or region (ibid.). In contrast, relational community refers to communities of interests such as hobby clubs, religious groups etc., and tends to be concerned with the quality and character of human relations, without necessarily referring to a geographic location (Obst *et al.* 2002). Interestingly enough, in trying to provide various representations of 'community', Obst *et al.* (2002) borrows the discussion of the concept from the field of community psychology. They allude to 'the psychological sense of community (PSOC)', which was introduced by Sarason in 1977, a concept that expounds on the relational definition of community. According to these authors, characteristics of a sense of community include,

> (1) perceptions of similarity with others;
> (2) acknowledgment of being interdependent with other people;
> (3) willingness to act in ways that maintain this interdependency; and
> (4) having a sense of belonging to a larger, dependable and stable structure.

Norris, Stevens, Pfefferbaum, Wyche, and Pfefferbaum (2008: 139) define the sense of community as 'an attitude of bonding that includes mutual concerns and shared values and that are characteristic of resilient communities'. Amongst researchers who investigated the theoretical frameworks under-

pinning PSOC, are McMillan and Chavis (1986) who advance four dimensions of PSOC, viz. membership, influence, integration, fulfillment of needs, and shared emotional connection.

Representations of 'community' from both community psychology and community engagement have a shared meaning – both in terms of its varied nature and its definitions, albeit nuanced differences as articulated within the community psychology field/approach. In the discussion we noted how community engagement borrowed concepts from community psychology to clarify their understanding of the concept 'community'. To a greater extent, community psychology aligns the representation(s) of the concept to factors associated with the emergence of the sub-discipline/approach – as a critique to mainstream psychology and as located within the socio-political space. This alignment results in community psychology adopting a subjective stance in its conceptualisation of the concept. Definitions of 'community' in community engagement denote community as a concept that is 'out there' and which can be studied outside of the individual/group/community, adopting a value-free, if not an objective stance in its explanation of the concept. At this point, I raise the question: 'does the adoption of a particular stance in the understanding of the concept 'community' affect how we engage with communities?' Will this effect influence communities' sense of control over their environment and their feelings of confidence from fear?

In the sections that follow, I explore how communities are engaged with, in community engagement, in an attempt to answer these questions.

## *3.2 The Practice of Community Engagement*

The Practice Notice document presents a founding principle upon which the practice of community engagement in peacekeeping should be understood, viz, 'politics must drive the design and implementation of peace operations' mandate' (DPKO/DFS 2018: 5). The assumption here is that the local community should be allowed to influence the design of peacekeeping strategies.

As a point of departure, the Practice Note emphasizes inclusive peacekeeping, which incorporates a participatory political dialogue. The aim of this dialogue is to promote the shared understanding of goals between key role-players – in this instance, the affected stakeholders, communities, and the UN and its partners. This principle aims to safeguard the interest of the community against exclusionary processes that may result from insensitivity [to critical

issues and/or processes] on the part of those leading peace processes. When engaging with communities, it is essential to avoid using a top-down approach that may not ensure engagement with trusted national authorities and interlocutors; including consideration of all root causes of conflict that the community may perceive as urgent (DPKO/DFS 2018). Another consideration in the community engagement process is the inclusion of unpopular and difficult community issues that run the risk of being omitted when marginalized voices are excluded from the engagement process.

Rupesinghe (2016) shares three key goals of engagement, viz. communication, consultation, and empowerment. She explains that communication ensures communities receive the necessary information that will enable them to organize themselves. On the other hand, consultation enables communities to share their perspectives, grievances, needs, and priorities with peacekeepers [for the purpose of designing and developing relevant and appropriate interventions]. Lastly, empowerment allows communities to be directly involved in decision-making processes.

The principle stated above, and its aim within community engagement seeks to promote consultation and to allow the voice of the community [both prominent and marginalized] to be heard. In this respect, community engagement operates on similar principles to those of community psychology, particularly at the level of promoting and encouraging participation, collaboration, and empowerment. As communities share their local security concerns and are given the opportunity to prioritize them, they feel empowered to influence how peacekeeping is managed and implemented [in their own communities]. Henigson (2020) advances three main reasons why the UN Peacekeeping engages with communities:

1. To sensitize local communities on their mandate and to manage community expectations about their role of peacekeeping as well as build relationships with the communities
2. To understand the potential threats facing local communities from the perspective of communities and to also obtain information on existing community-based, self-protection mechanisms.
3. To support the resolution of localized conflicts and to build protective environments

Furthermore, Henigson (2020) described three main areas of focus for community engagement, depicted in Table 2 below.

| Activity | Civilian Component | Military Component | Police Component |
|---|---|---|---|
| **Awareness-raising, information-sharing, and relationship building** | • Meetings with local communities to sensitize them to the mission mandate<br>• Information sharing through activities such as public events, radio shows, or the use of social media | • Informal engagement with community members during dismounted patrols<br>• Meetings with local communities in hotspots to sensitize them to the mission mandate | • Informal engagement with community members during dismounted patrols<br>• Information sharing in community meetings<br>• Meetings with local communities in hotspots to sensitize them to the mission mandate |
| **Conflict resolution and reconciliation and community-level peacebuilding** | • Facilitation of inter-community meetings to mediate conflict<br>• Capacity-building workshops with civil society organizations or community-level groups and actors | • Support to local conflict-resolution and reconciliation efforts, usually in coordination with civilian sections<br>• Support for quick impact projects, usually in coordination with civilian sections | • Efforts to build community-level trust in the national police<br>• Support to local conflict-mediation efforts<br>• Capacity-building support to strengthen community members' self- |

| | | | |
|---|---|---|---|
| | • Disarmament, demobilization, and reintegration (DDR) and community violence reduction (CVR) programming<br>• Quick-impact projects | • Facilitation of dialogue between host-state security forces and local communities | protection measures |

**Table 2. Community engagement activities (Henigson 2020)**

Key principles of community psychology are collaboration, participation, and empowerment (Carolissen *et al.* 2010; Naidoo 2000; Perkins & Zimmerman 1997; Rappaport 1981; Yen 2007). There is an immediate link between community engagement in peacekeeping and community psychology as both emphasize the critical role played by collaboration and participation in promoting ownership [amongst communities], with a view to empowering community members. Peacekeeping that is focused on the local context is concerned with understanding drivers of conflict from the perspective of community members and thereafter, customizing their overall mandated tasks (DPKO/DFS 2018). The assumption in this approach is that, these drivers of conflict are found within local communities, hence communities are regarded as experts in determining these drivers. It is not clear whether the inherent socio-political environment is taken into consideration during this information-gathering process. However, studies that focus on peace, women, and security (PWS) provide a sense that the broader socio-political environment is considered when designing peace operations (Donais & Murray 2021; Holmes 2020; Klossek & Johansson-Nogues 2021; Nagel, Fin & Maenza 2021). With these emerging studies, it seems more likely that, similar to the Social Action model of community psychology, there is a deliberate attempt to mobilize community members into collective action against problematic societal structures (Butchart & Seedat 1990). Such efforts serve to transform communities (Ngonyama ka Sigogo *et al.* 2007) and are in keeping with the

goal of community psychology, which is to radically transform and redefine the profession of psychology whilst serving the historically oppressed (Seedat, Duncan & Lazarus 2001).

Community within community engagement has been demonstrated to adopt an objective or value-free stance, unlike community psychology, which adopted a subjective stance in its representation of 'community'. From the analysis provided in the foregoing discussions, a subjective stance to 'community' resulted in an explicit understanding of the objective of community psychology as transformative. On the other hand, in line with its objective or value-free stance, community engagement [as reflected in the Practice Note] is silent on its transformative agenda, this agenda only emerges in studies conducted post the release of the Practice Note, as a way of applying it. Given the value of transformation on communities, it would benefit community engagement to explicitly declare its stance in defining the concept of 'community'. This objective or value free stance is commensurate with the less progressive and less transformative community consultations and participation. One can assume that a community that is engaged in a less transformative consultation and participation process is less likely to feel a sense of control over their environment and may experience lower feelings of confidence from fear.

Another key theme in the practice of community engagement involves its use of models or theoretical frameworks. While the Practice Note offers in-depth discussions of processes to be followed when engaging communities, it does not particularly offer any theoretical models that should be used for this engagement. After all, community engagement is defined as 'a strategic *process* that involves local populations in all aspects of decision-making, policy development, and implementation to strengthen local ownership, capacities and community structures as well as to improve transparency, accountability and optimal resource allocations across diverse settings' (UN 2020: 5). This implies that community engagement does not seem to be based on a well-defined theoretical framework. While the United Nations Department of Peace Operations (UN DPO 2020) mentions the different tools used in community engagement, viz., Community Liaison Assistants (CLAs), Community Alert Networks (CANs), Joint Protection Teams (JPTs), Joint Assessment Missions (JAMs), Community Protection Plans (CPPs) Community Oriented Policing (CoP), the theoretical basis for this is not presented. Similarly, while processes for engaging communities within peacekeeping were advanced, these were devoid of a theoretical framework or model.

In contrast, community psychology, as presented in section 3 above, is practiced within either the mental health, social action, ecological, and/or organizational models. The discussion (in section 3 above) indicated how each model explains and resolves mental health issues within communities. I argue that the practice of community engagement in peacekeeping could benefit from developing a model (s) of community engagement so as to offer theoretical understandings of how various concepts [used in community engagement] interact to explain specific phenomena – e.g. in understanding and implementing the processes for community engagement as explained in the Practice Note, is there a specific sequence through which these processes occur? What happens if any of the processes that were explained does not take place? In what way would this affect the overall goal of the process? Gaining insight from other contexts that also utilize community engagement, Abimbola (2019) reflects on how she was compelled to develop a theory for community engagement after noticing gaps that existed in systematic and theory-driven policies [going beyond merely describing that things are (not) happening to provide answers to questions that ask why things are (not) happening]. The use of theory in community engagement is not uncommon, as will be illustrated in the section that follows, where community engagement has been applied in settings other than the military.

Community engagement [as a practice] has been applied in various contexts, including [but not limited] to learning, higher education, public health, research, and various disciplines such as Archeology, Psychology, and Nursing, to name a few (Abimbola 2019; Brunton, Thomas, O'Mara-Eves, Jamal, Oliver & Kacanagh 2017; De Leiuen & Arthure 2016; Ebersohn, Bender & Carvhalho-Malekane 2010; France-Harris, Burton & Mooney 2019; Rutty 1998; South & Phillips 2014; Zuber-Skerritt 2015). In all these contexts, its practice is based on a particular model or theoretical framework. A few of these include the Participatory Action Learning and Action Research theoretical framework (PALAR) (Zuber-Skerritt 2015), International Association for Public Participation (IAP2) community engagement model (De Leiuen & Athure 2016), the Experiential Learning model (Ebersohn *et al.* 2010) and AT-EASE model (France-Harris *et al.* 2019).

Other studies present justifiable arguments for the use of theoretical frameworks in understanding the link and impact of community engagement on behaviour, especially within the public health domain (Abimola 2019; Brunton *et al.* 2017; South & Phillips 2014). Illustrating one such argument, Abimola (2019) is of the view that the contextual circumstances that are linked to the

performance of community health committees lack a theoretical basis. In a similar vein, Brunton *et al.* (2017) argue that it is necessary to understand relationships between concepts. They cite the following example: '…we needed to consider how a process of collective decision-making influenced people's motivations for engagement and how this, in turn, might lead to particular outcomes including harms – for example – disillusionment when expectations were not met' (p. 3). The above discussions have provided justification for the development of a community engagement theory for peacekeeping.

I further argue that community engagement within the context of peacekeeping could find some of the community psychology models useful, particularly as the two fields intersect in many respects. As a starting point, community engagement needs to clarify its use of the concept 'empowerment'. Section 3.3 below delves into the use of empowerment in the practice of community engagement in peacekeeping. Case examples from the implementation of community engagement in peacekeeping, as contained in the handbook on 'protection of civilian in United Nations peacekeeping' (UN DPO 2020) provides examples of how community consultation processes resulted in empowerment of communities. The handbook clearly provides best practices in the implementation of community engagement, following the publication of the Practice Note. These positive developments could be used to assist in redefining the use of the concept [empowerment] in community engagement.

Ngonyama ka Sigogo *et al.*, (2004) argue that the Social Action model [in community psychology] advances a transformative agenda because of its focus on the radical transformation of social problems (Butchart & Seedat 1999). Applying the Social Action model in community engagement can assist the practice of community engagement to understand the relationship between their key concepts and how this relationship contributes to empowerment or transformation of communities.

## *3.3 Attainment of Psychological Security in Community Engagement*

The Practice Note presents best practices on how to engage with communities in peacekeeping. Detailed steps to be followed as well as their intended outcome at any given phase of the process are provided. There are three main processes that are involved when engaging communities for peacekeeping – consultation, goal-setting, and communication. The main purpose of consulting with communities is to create clear and effective community entry points and to develop

clear and usable feedback for peace operations (DPKO/DFS 2018). Once feedback has been received from community members, the next process requires setting goals to ensure community priorities are incorporated into the peacekeeping plan (DPKO/DFS 2018). Communication is another central process that is emphasized in community engagement (DPKO/DFS 2018).

These best practices provide a systematic and coherent process for engaging communities. I discuss focal points for each of these best practices in the sections that follow.

The Practice Note argues for some level of coherence between these processes for them to be effective. *Consultation* entails the mapping of stakeholders and the building of relationships. There is also sharing of information on specific drivers of conflict and analysis and reporting of the shared information. A key requirement of the consultation process is to strive for inclusivity in stakeholder representation.

The *goal-setting* process entails setting internal priorities, shaping political processes, and managing risks. While peacekeeping has its own priorities, viz. restoring state authority; disarmament, demobilization, and reintegration (DDR), including community violence reduction; support to judicial and penal institutions; and security sector reform (DPKO/DFS 2018), it needs to equally consider the priorities identified by the community. The Practice Note highlights two main challenges that impact the success of this process. The first one concerns the integration of community priorities and drivers of conflict into the peacekeeping mission's overall mandated tasks. The second one refers to the use of UN resources – material and technical, to ensure alignment between political and peace processes, as well as community priorities. The goal-setting process is primarily about ensuring communities are given a voice and this voice is heard, during peacekeeping decision-making, to ensure the relevance and responsiveness of interventions.

The last process for engaging with communities is *communication*. The Practice Note premises the importance of effective, outward communication on the following 2008 guiding principle:

> If the parameters of United Nations activity are clearly laid out and explained to the local population and other target audiences, fear and misunderstanding will be minimized, disinformation will be corrected, and the impact of those who wish to damage the peace process through rumor and untruth will be minimized.

At the same time, the Practice Note admits the complexities surrounding communication in peacekeeping. The first of these has to do with an outdated communication model, which is labeled as best practice. The second entails acknowledgment of the multi-dimensional nature of the peace process, with multiple stakeholders, each having their own interests and communication strategies for influencing individual events. This, renders coherence in communication channels difficult.

Mindful of the above challenges, the Practice Note emphasizes the importance of good strategic communication, community links, and management of crises and rumors. Timely and accurate information strengthens strategic communication.

The processes that were outlined above have illustrated the extent to which community engagement seeks to reach out to communities, and empower them to take ownership of their peacekeeping, by including all types of voices [prominent, marginalized, mainstream, silenced etc.] and removing any misconceptions about aspects related to peacekeeping. A framework for implementing these processes has also been clearly mapped out, to provide guidance and avoid confusion within the sector. These processes resonate with most community psychology processes. Both fields/approaches emphasize inclusive, bottom-up approaches that lead to community empowerment.

Empowerment is defined by the Cornell Empowerment Group as: 'an intentional ongoing process centered in the local community, involving mutual respect, caring and group participation through which people lacking an equal share of valued resources gain greater access to and control over those resources' (cited in Perkins & Zimmerman 1995). Another definition by Rappaport (1987) refers to a process through which people gain control over their lives, and democratically participate in the life of their community. The definition by the Cornell Empowerment Group indicates that processes used for community engagement in peacekeeping, possibly lead to partial empowerment of the community. There is indeed an intentional process that is centered in the community which involves mutual respect, critical reflection [although not explicit], and group participation as reflected in both the consultation and goal-setting processes of community engagement. An empowerment aspect that is not explicitly evident from the processes of community engagement relates to the 'intentional *ongoing process*'. While the process of consultation is centered in the local community, there is no reference to an ongoing process, post-implementation of the peacekeeping strategy. In this sense, empowerment doesn't seem to be sustained over time, which may raise questions of whether

this constitutes true empowerment that leads to liberation. A second empowerment aspect that is hidden from the community engagement processes relates to '… *people lacking an equal share of valued resources gain greater access to and control over the resources*'. Participation of community members in peacekeeping seems limited to consultation and goal-setting processes, there is no reference to any access to and control over valued resources. Again, this points to possible, partial empowerment of the community. Applying Rappaport's definition of empowerment to community engagement yields similar results. There is no clear indication of '*people gaining control over their lives*' as a result of having participated in the above-discussed processes of consultation and goal-setting.

The above analysis yet again confirms the assertion that the representation of community and how communities are positioned have a bearing on how each field/approach engages with its community. While engaging the community in peacekeeping as per the processes outlined in this section may empower communities to make decisions that inform peacekeeping strategies [for their own communities], it is not clear if this process impacts communities' sense of liberation and transformation. The definitions of empowerment and psychological security all point to: 'control over one's life'. At phase value, one can assume that if individuals feel empowered, they would more likely perceive the environment as providing psychological security. Linking this to psychological security, it is unclear whether community members would regard themselves as having a sense of control over their social environment when they are regarded as not being fully empowered.

## 4 Conclusion

This article explored the practice of community engagement in providing psychological security of communities in peacekeeping, using community psychology as a conceptual framework. The study adopted Maslow's definition of psychological security, as referring to communities' sense of control over their environment, including their feelings of confidence from fear. The study argued that psychological security, within peacekeeping, is dependent upon conscious and active participation of communities for which safety is required. The study, further argued that representations of community and positions adopted in understanding this concept, have a bearing on how communities are engaged. By exploring the practice of community engagement, the study revealed how a subjective representation of community is associated with community

empowerment, while an objective or value free representation of community is associated with a partially empowered community. When communities feel empowered through participating meaningfully in decision making processes and having a sense of sustained control over their environment, they are more likely to perceive as sense of psychological security.

Community engagement as a practice in peacekeeping:

1. Is a process that attempts to meaningfully engage communities to shape their own safety and security – responsibility for meaningful and contextual solutions are not determined externally, but the community is given agency [be it at a very basic level]

2. Attempts to shift from understanding security as an objective concept [which can be provided to people] to understanding security as a subjective concept [which results from considering collective community perceptions of what can lead to security] (Bar-Tal & Jacobsen 1998).

This study concludes with the following recommendations, which serve to better clarify or improve the practice of community engagement in peacekeeping:

- It is necessary for the community engagement practice to reconsider its positioning of the concept 'community'. Currently the Practice Note framework is not explicit about this positioning. In line with the assertion of this study, representations of the concept have a bearing on how communities are engaged with and subsequently impact on communities' perceptions of psychological security.

- The manner in which the concept 'empowerment' is discussed and applied in the Practice Note, does not fully align with the community psychology conceptual framework that was used for this study. It is thus recommended that the concept be explained in relation to its transformational/liberatory agenda. As a starting point, it may be useful to conduct empirical research to understand the consultation processes used in community engagement, the power dynamics inherent within communities during this process and the resultant [personal] impact of

the consultation processes on community members, in order to get the extent of the process' empowerment effect.

- The study has shown how the Practice Note is silent on models or theoretical frameworks for community engagement. The study has furthermore illustrated how studies that applied community engagement argued for the use of theory and even applied theory. This study therefore recommends that such theory be developed to guide the practice of community engagement in peacekeeping. This, for instance would allow for deeper understandings of how empowerment is achieved and explained. A starting point might be to conduct systematic literature reviews of all studies related to community engagement within the peacekeeping context, to assess for theoretical grounding.

I acknowledge that this study has its limitations. The main limitation being exclusive focus on the Practice Note, as a basis for the discussion of community engagement.

## References

Abimbola, S. 2019. Beyond Positive 'a priori' Bias: Reframing Community Engagement in LMICs. *Health Promotion International* 1 - 2. Available at: https://doi.org/10.1093/heapro/daz023 PMid:30982066 (Accessed on 05 February 2023.)

Bar-Tal, D. & D. Jacobsen 1998. A Psychological Perspective on Security. *Applied Psychology: An International Review* 47, 1: 59 – 71. Available at: https://doi.org/10.1111/j.1464 - 0597.1998.tb00013.x (Accessed on 14 April 2023.) https://doi.org/10.1080/026999498378079

Baxter, P. & S. Jack 2008. Qualitative Case Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report* 13, 4: 544 - 559. Available at: http://www.nova.edu/sss/QR13-4/baxter.pdf

Berger, S. & S. Lazarus 1987. The Views of Community Organisers on the Relevance of Psychological Practice in South Africa. *Psychology in Society* 7: 2 - 6.

Brunton, G., J. Thomas, A. O'Mara-Eves, F. Jamal, S. Oliver & J. Kavanagh 2017. Narratives of Community Engagement: A Systematic Review-

derived Conceptual Framework for Public Health Intervention. *BMC Public Health* 17, 1: 1 - 15. https://bmcpublichealth.biomedcentral.com/articles/10.1186/s12889-017-4958-4 (Accessed on 06 February 2023.) https://doi.org/10.1186/s12889 - 017 - 4958 - 4 PMid:29228932 PMCid:PMC5725895

Butchart, A. & M. Seedat 1990. Within and Without: Images of Community and Implications for South African Psychology. *Social Sciences Medicine* 31,10: 1093 - 1102. https://doi.org/10.1016/0277 - 9536(90)90231 - G

Carolissen, R., P. Rohleder, V. Bozalek, L. Swartz & B. Leibowitz 2010. Community Psychology is for Poor, Black People. Pedagogy and Teaching of Community Psychology in South Africa. *Equity and Excellence in Education* 43, 4: 495 – 510. Available at: https://www.tandfonline.com/loi/ueee20 (Accessed on 30 January 2023.) https://doi.org/10.1080/10665684.2010.516695

Cummings, E.M. & L.E. Miller-Graff 2015. Emotional Security Theory: An Emerging Theoretical Model for Youth's Psychological and Physiological Responses across Multiple Developmental Contexts. *Current Directions in Psychological Science* 24, 3: 208 – 213. Available at: https://doi.org/10.1177/0963721414561510 (Accessed on 18 February 2023.)

Dawes, A. 1986. The Notion of Relevant Psychology with Particular Reference to Africanist Pragmatic Initiatives. *Psychology in Society* 5: 2848.

De Leiuen, C. & S. Arthure 2016. Collaboration on Whose Terms? Using the IAP2 Community Engagement Model for Archeology in Kapunda, Australia. *South Australia Journal of Community Archeology & Heritage* 3, 2: 81 - 98. Available at: http://www.tandfonline.com/loi/ycah20 (Accessed on 05 February 2023.) https://doi.org/10.1080/20518196.2016.1154735

Donais. T. & S. Murray 2021. Gender and Protection in UN Peacekeeping: towards Inclusive Protection Practice. *Balsille Papers* 4,1: 1 - 12. https://doi.org/10.51644/BAP41

Department of Peacekeeping Operations – Department of Field Support (DPKO/DFS) 2018. *Peacekeeping Practice Note: Community Engagement*. United Nations Peacekeeping.

Ebersohn, L., C.J.G. Bender & W.M. Carvhalho-Malekane 2010. Informing Educational Psychology Training with Students' Community Engagement Experiences. *Perspectives in Education* 28, 3: 87 – 98.

France-Harris, A., C. Burton & M. Mooney 2019. Putting Theory into Practice: Incorporating a Community Engagement Model into Online Pre-professional Courses in Legal Studies and Human Resource Management. *Online Learning* 23, 2: 21 - 39 Available at: https://doi.org/10.24059/olj.v23i2.1448 (Accessed on 05 February 2023.)

Gerring, J. 2004. What is a Case Study and What is it good For? *American Political Science Review* 98, 2: 341 - 354. https://doi.org/10.1017/S0003055404001182

Gizelis,T., H. Dorussen & M. Petrova 2016. Research Findings on the Evolution of Peacekeeping. *Oxford Research Encyclopaedia of Politics.* https://doi.org/10.1093/acrefore/9780190228637.013.25

Gordon, G.M. & L.E. Young 2019. Cooperation, Information, and Keeping the Peace: Civil Engagement with Peacekeepers in Haiti. *Journal of Peace Research* 54, 1: 64 - 79. Available at: https://doi.org/10.1177/0022343316682063 (Accessed on 30 January 2023.)

Gorur, A. & N. Carstensen 2016. Community Self-protection. In Willmot, H., R. Mamiya, S. Sheeran & M. Weller (eds.): *Protection of Civilians.* Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198729266.003.0020

Gouling, M. 1993. The Evolution of United Nations Peacekeeping. *International Affairs* 69,3: 451 - 464. https://doi.org/10.2307/2622309

Henigson, H. 2020. Community Engagement in United Nations Peacekeeping Operations: A People-centred Approach to Protecting Civilians. *International Peace Institute*. Available at www.ipinst.org (Accessed on 27 January 2023.)

Holmes, G. 2020. Strengthening UK Support for Gender-responsive, People-centred Peacekeeping in Africa. *The RUSI Journal* 165,5 - 6: 36 - 45. https://doi.org/10.1080/03071847.2020.1844593

Hultman, N., J. Kathman & M. Shannon 2013. United Nations Peacekeeping and Civilian Protection in Civil War. American *Journal of Political Science* 57, 4: 875 – 891. Available at: https://doi.org/10.1111/ajps.12036 (Accessed on 30 January 2023.) https://doi.org/10.1111/ajps.12036

Jia, J.C., D.P. Li, X. Li, Y. Zhou, Y. Wang, W. Sun & L. Zhao 2018. Peer Victimization and Adolescent Internet Addiction: The Mediating Role of Psychological Security and the Moderating Role of Teacher - Student

Relationships. *Computers in Human Behavavior* 85: 116 - 124. https://doi.org/10.1016/j.chb.2018.03.042

Julian, R. & C. Schweitzer 2015. The Origins and Development of Unarmed Civilian Peacekeeping. *Peace Review: A Journal of Social Science* 27: 1 - 8. Available at: https://www.tandfonline.com/loi/cper20 (Accessed on 26 January 2023.) https://doi.org/10.1080/10402659.2015.1000181

Klossek, L. & E. Johansson-Nogues 2021. The Female Boot on the Ground: Indian Ambivalence over Gender Mainstreaming in United Nations Peacekeeping Operations. *International Peacekeeping* 28, 4: 527 – 552. Available at https://doi.org/10.1080/13533312.2021.1880899 (Accessed on 07 February 2023.)

Krishnan, S. 2020. United Nations Peacekeeping, Responsibilities to Protect and Humanitarian Interventions. *India Quarterly* 76, 1: 120 - 135**.** Available at: https://doi.org/10.1177/0974928419901198 (Accessed on 30 January 2023.)

McMillan, D.W & D.M. Chavis 1986. Sense of Community: A Definition and Theory. *Journal of Community Psychology* 14: 6 - 23. https://doi.org/10.1002/1520 - 6629(198601)14:1<6::AID - JCOP2290140103>3.0.CO;2 - I

Nagel, R.U., K. Fin & J. Maenza 2021. *Peacekeeping Operations and Gender: Policies for Improvement: Policy Brief*. Canada: Georgetown Institute for Women, Peace and Security.

Naidoo, V.A. 2000. *Community Psychology: Constructing Community, Reconstructing Psychology in South Africa*. Inaugural Address. Stellenbosch University, Stellenbosch.

Ngonyama ka Sigogo, T., M. Hooper, C. Long, M.B. Lykes, K. Wilson & E. Zietkiewicz 2004. Chasing Rainbow Notions: Enacting Community Psychology in the Classroom and Beyond in Post-1994 South Africa. *American Journal of Community Psychology* 33, 1/2: 77 - 89. https://doi.org/10.1023/B:AJCP.0000014320.65759.a5 PMid:15055756

Norris, F., S. Stevens, B. Pfefferbaum, K. Wyche & R. Pfefferbaum 2008. Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness. *American Journal of Community Psychology* 41,1-2: 1573 - 2770. https://doi.org/10.1007/s10464 - 007 - 9156 - 6 PMid:18157631

Obst, P., L. Zinkiewics & S.G. Smith 2002. Sense of Community in Science Fiction Fandom, Part 1: Understanding Sense of Community in an International Community of Interest. *Journal of Community Psychology* 30, 1: 87 - 103. https://doi.org/10.1002/jcop.1052

Perkins, D.D. & M.A. Zimmerman 1997. Empowerment Theory, Research and Application. *American Journal of Community Psychology* 23,5: 569 - 579. https://doi.org/10.1007/BF02506982 PMid:8851340

Rappaport, J. 1981. In Praise of Paradox: A Social Policy of Empowerment over Prevention. *American Journal of Community Psychology* 9: 1 - 25. https://doi.org/10.1007/BF00896357 PMid:7223726

Rupesinghe, N. 2016. Strengthening Community Engagement in United Nations Peace Operations. *Conflict & Resilience Monitor* 3.

Rutty, J.E. 1998. The Nature of Philosophy of Science, Theory and Knowledge Relating to Nursing and Professionalism. *Journal of Advanced Nursing* 28, 2: 243 - 250. https://doi.org/10.1046/j.1365 - 2648.1998.00795.x PMid:9725719

Seedat, M., N. Cloete & I. Shochet 1988. Community Psychology: Panic or Panacea. *Psychology in Societ*y 11: 39 - 54.

Seedat, M., N. Duncan & S. Lazarus (eds.). 2001. *Community Psychology. Theory, Method and Practice. South African and Other Perspectives*. Cape Town: Oxford University Press.

Seedat, M. & S. Lazarus 2011. Community Psychology in South Africa: Origins, Developments and Manifestations. *Journal of Community Psychology* 39, 3: 241 - 257. https://doi.org/10.1002/jcop.20429

Seedat, M. & S. Lazarus 2014. Community Psychology in South Africa: Origins, Developments and Manifestations. *South African Journal of Psychology* 44,3: 267 - 281. Available at: https://doi.org/10.1177/0081246314537431 (Accessed 01 February 2023.)

Singh, G. 2020. Protection of Civilians: United Nations Peace-keepig Missions in the Democratic Republic of Congo and Republic of South Sudan. *Manekshaw Paper 88*. https://doi.org/10.18356/9789210056755c047

South, J. & G. Phillips 2014. Evaluating Community Engagement as Part of the Public Health System. *Journal of Epidemiol Community Health* 68, 696 - 69. https://doi.org/10.1136/jech - 2013 - 203742 PMid:24671849

United Nations Department of Peace Operations UN DPO 2020. *The Protection of Civilians in United Nations Peacekeeping.* Handbook. United Nations.

Yen, J. 2007. A History of 'community' and 'community psychology' in South Africa. In Duncan, N., B. Bowman, A. Naidoo, J. Pillay & V. Ross (eds.): *Community Psychology: Analysis, Context and Action.* Cape Town, South Africa: UCT Press.

Zotova, O.Y & L.V. Karapetyan 2018. Psychological Security as the Foundation of Personal Psychological Wellbeing: An Analytical Review. *Psychology in Russia: State of the Art* 11,2: 100 - 113. Available at: http://psychologyinrussia.com (Accessed on 15 April 2023.) https://doi.org/10.11621/pir.2018.0208

Zuber - Skerritt, O. 2015. Participatory Action Learning and Action Research (PALAR) for Community Engagement – A Theoretical Framework. *Educational Research for Social Change ERSC* 4,1: 5 - 25.

Matshepo Matoane
School of Applied Human Sciences
University of Kwa-Zulu Natal
South Africa
Matoanem@ukzn.ac.za

# Chapter 18: The Mistakes Made in Response to the COVID-19 Pandemic: How to Deal with Future Pandemics

**Gert Kruger**
**ORCID iD: https://orcid. org/0000-0003-0606-2053.**

**Colleen Aldous**
**ORCID iD: https://orcid. org/0000-0002-7199-9160.**

## Abstract
The COVID-19 pandemic, caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), swiftly became a global crisis, prompting the World Health Organization (WHO) to declare it a pandemic in March 2020. Over the following two years, the virus evolved, leading to numerous waves of infections and the emergence of the omicron variant by December 2021. The pandemic had profound impacts on healthcare, the economy, education, and public trust in 'science', the media and the authorities. This paper explores the mistakes made during the COVID-19 response and seeks ways to enhance future pandemic preparedness.

**Keywords**: COVID-19 pandemic, Lockdowns, Evidence-based medicine (T-EBM Wheel), Holistic Management, Ivermectin, Pharmaceutical conflicts of interest

## Overview of the Pandemic and its Impact
The COVID-19 pandemic was portrayed as a once-in-a-century global infectious disease health crisis caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) (Cruickshank & Shaban 2020). It is documented to have first been identified in Wuhan, China, in December 2019 and then spread rapidly worldwide. By March 2020, the WHO declared COVID-19 to be a pan-

demic, a response thought by many to have been slow (Zhou, Zhang & Qu 2020). From 2020, waves of the disease, driven by mutations in the virus, continued to spread across the globe with serious health consequences for two years (Van Damme 2020). By December 2021, the omicron variant began replacing most previously circulating variants, and the disease has become less severe and endemic (Markov *et al.* 2023). By July 2023, SARS-CoV-2 had infected 767,972,961 people and killed 6,950,655 people (WHO 2023). It is important to note strong arguments exist that claim there was no Covid pandemic (Panda 2023).

The handling of COVID-19 impacted all aspects of life, from healthcare, the economy, education, and social interaction to public trust in the mainstream narrative that was created by the various authorities. Its impact on the health systems was the most obvious but possibly not the most significant. Shortages of medical supplies, including personal protective equipment for staff (PEP) equipment for patients such as ventilators, therapeutics, and medical staff, may have resulted in higher mortality among vulnerable patient groups such as geriatric patients and those with chronic health conditions (Jakovljevic *et al.* 2020). Mortality rates up to 90% were reported (Yang *et al.* 2020; Richardson *et al.* 2020) for COVID patients on ventilators largely due to Ventilator-Associated Pneumoni (Wicky *et al.* 2023). Some debate is ongoing about whether mechanical ventilation is a suitable treatment for may Covid patients (Ducharme 2020).

Possibly the most serious impact of the pandemic was on the economy. Lockdowns caused businesses across both the formal and informal sectors to suffer financial losses that led to the closure of many companies and small businesses and the consequent loss of jobs. Ironically, the salaries of politicians imposing harsh lockdowns were secured. Consumer spending fell sharply as a result, which scaled up to countries experiencing declines in their gross domestic product (GDP) and increases in unemployment rates. The global scale of this impact on business led to a worldwide recession (Ozili 2020).

Numerous significant research reports have underscored the substantial economic toll induced by the lockdowns implemented globally during the pandemic (Bhattacharya, Smark & Mir 2021; Rimšēvičs 2021; Meng, Bannerman & Abrokwah 2022). Reports emanating from every continent demonstrate this trend, presenting data that spans a wide array of economic sectors (S. Bhattacharya, Smark & Mir 2021; Chen *et al.* 2022; Fisher *et al.* 2022; Garcia, Thierry, and Pendergrast 2022; Morsy, Balma, and Mukasa 2021; Verschuur, Koks, and Hall 2021; Zhou, Zhang, and Qu 2020; Wu 2022; Zinecker *et al.* 2021).

In the United States, an analysis determined that, on average, the economic sacrifice made to prevent a single new COVID-19 infection was roughly $28,000, a figure reflected in the lower gross domestic product (GDP) (Tellis 2023). This substantial cost raises questions regarding the economic viability of stringent lockdown measures, inviting reflection on the strategies deployed to manage the pandemic and their repercussions on the economy.

During the lockdowns, educational institutions, including schools and universities, either shut their doors or adopted online learning platforms, resulting in widespread disruptions to the education of millions of students at diverse stages of their developmental progress. The lockdowns showed stark contrasts in accessibility to education, with affluent institutions swiftly adapting to the changes, in contrast to schools situated in underserved communities that lacked the necessary resources to facilitate online learning (Spaull & van der Berg 2020). Recently a court ordered Johns Hopkins University to refund students for remote learning during the pandemic (Staff 2024).

Despite being a viable alternative, remote learning could not fully replicate the rich, multifaceted social experiences that traditional in-person learning offers, especially for programs necessitating laboratory practicals. This discrepancy shows that the ramifications of the educational disruptions caused by the COVID-19 lockdowns were far-reaching, and their full extent may only unfold over the coming decades.

Given this landscape, it is imperative for societies globally to engage in critical reflection on the scope of authority, including emergency powers, that they are willing to allocate to governmental bodies. This discussion should encompass the broader implications of such decisions, considering the potential for profound impacts on fundamental aspects of society, such as education.

Social distancing measures were implemented to slow the spread of the disease and had mixed impacts. People who lived alone or were isolated from their families, such as those who lived in facilities for older people, had increased feelings of isolation and loneliness. Children were denied face-to-face contact with peers for extended periods, leading to feelings of isolation. Developmental milestones in communication, emotional regulation, and socialisation were compromised (Spaull & van der Berg 2020).

Media threads and information blackouts due to government censorship (Bhattacharya 2023; Showalter 2023; Kenny 2023; Team 2023; Christenson 2023; Prasad 2020) worldwide, impacted public trust in science and the authorities. There was high public trust in science and scientists at the beginning of the pandemic. Governments and individuals looked to a handful of experts,

mainly from clinical research and practice backgrounds, to guide them through the crisis. However, as the pandemic progressed, trust in science became more polarised, with some becoming more sceptical of scientific information and advice sources. This was partly due to conflicting information and guidance from different sources and some countries' politicisation and propaganda of the pandemic response. The rapid pace of scientific research and development of vaccines, treatments, and diagnostic tools led to concerns about the safety and efficacy of these interventions. Some sources' blatant untruths raised suspicions, leading to further misgivings about science (Mannan 2020).

During the COVID-19 pandemic, a vigorous media campaign arose, casting doubt on the efficacy of ivermectin and hydroxychloroquine as treatments for the virus, a discourse fuelled by various studies and analyses over time (Todaro 2020; Darcy 2022). However, more recent research suggests a potential effectiveness of ivermectin in treating COVID-19 (Bryant *et al.* 2021).

Controversies have erupted regarding the perceived compromise of organisations such as the WHO and the FDA, stemming from the substantial funding they receive from the pharmaceutical industry. The WHO's 2022-23 budget prominently features voluntary contributions, eclipsing the funds allocated by member states by a significant margin; in 2020, a notable part of these contributions was derived from the pharmaceutical sector (WHO 2020, 2023a). The FDA similarly has a considerable portion of its budget funded by the pharmaceutical industry, raising questions regarding potential conflicts of interest and the ability of the agency to regulate the industry impartially (Jewett 2020).

The pharmaceutical industry's influence extends further into the political landscape, with substantial lobbying efforts in the USA marking a continuous strategy to shape policy and public opinion (Secrets 2023b; 2023a). This deep-seated involvement has fostered a growing mistrust among the public, with the mainstream media reported to be significantly financially supported by the pharmaceutical industry, generating scepticism and fuelling polarisation across the political spectrum.

Lies about the effectiveness of the vaccines (Agresti 2022; Chongloi 2022; Lin 2022) and the masks (Hoeg, González-Dambrauskas & Prasad 2023; Jefferson *et al.* 2010; Kisielinski *et al.* 2023; Radonovich *et al.* 2019) contributed further towards mistrust of the public. We have recently published a comprehensive review on the adverse effects of the COVID-19 vaccines (du Preez *et al.* 2024). It is clear that the Pharmaceutical companies kept the initial negative results from the clinical trials secret (during the trials, more people that

were vaccinated died compared to those that were given placebo) at least to the public. The USA government tried to hide this information from the public for decades to come (Greene 2021; Deese 2022). Fortunately, the courts ruled in favour of a group of medical doctors and scientists that. used the Freedom of Information Act request to release the data (Deese 2022; Greene 2022). Another strategy that they used was to discredit the use of any alternative treatment (such as Ivermectin), as this would have destroyed their chances to obtain emergency approval for their COVID-19 vaccines (UPMC 2022). .

Another major contribution to the exploitation of people by Big Pharma developed when President Reagan signed a bill in 1986 that essentially exempted pharmaceutical companies from liability with respect to children vaccines (Spear 1986). It appears that the pharmaceutical companies obtained blanket exemption from liability from governments world-wide, with respect to the COVID-19 vaccines (Epstein 2022). Initially this fact was kept secret in most countries (Apuzzo 2021). The result is that people became much more sceptical about vaccines in general and subsequently more hesitant to use them, leading to a rise in vaccine-preventable diseases (Bassyouni 2024)

An urgent need exists to restore integrity and trust in the systems responsible for managing public health crises. It entails instituting measures to secure the independence of health service watchdogs, media, and industry regulators from potential conflicts of interest, ensuring transparency, and rebuilding public trust in these vital institutions. Liability of Pharmaceutical companies should be restored as well.

To achieve this, a multifaceted approach should be pursued involving stringent regulations on funding and lobbying, coupled with efforts to foster transparency and reduce the influence of financial contributions on decision-making processes. Moreover, promoting open dialogues grounded in verified scientific data and encouraging a culture of critical thinking can aid in combating misinformation and reducing political polarisation. Thus, a comprehensive reassessment and overhaul of the existing structures are called for to usher in an era where public health decisions are made to safeguard the populace's well-being, devoid of undue influences.

## The Importance of Examining Mistakes Made in Response to the Pandemic

The COVID-19 pandemic turned out to be the most significant health crisis of our time, albeit for the wrong reasons. Governments, healthcare organizations

and doctors on the ground responPded in various ways. Some actions restrained the disease, while others resulted in increased morbidity, mortality, and economic devastation. It is vital to examine the mistakes made and evaluate the successes to learn from them and take steps to address them. This way, we can better manage future similar crises more efficiently and not repeat the same mistakes.

The pandemic highlighted the need for preparedness and effective response strategies. Ironically, the only government that did followed experience from previous pandemics was Sweden. Although they were harshly criticized at the time, it turned out that they were actually right! (Andersson & Jonung 2024). Without reflecting on the mistakes made, it will be challenging to identify the most effective measures to use or avoid in the future. Governments and healthcare organisations should reflect critically on their responses to develop new policies and procedures to manage future outbreaks, leading to better health outcomes for the public.

Examining past responses and adjusting new response strategies might help restore public trust. Several reasons have led to the loss of public confidence in government-driven responses and healthcare institutions. Arguably, the most important has been the mis- and dis-information about evidence-based medicine propagated by authorities and some powerful individuals who became the pandem-icons (Joubert *et al.* 2023). By examining evidence more critically and allowing a comprehensive interpretation of evidence-based medicine to include the totality of the evidence, a rebuilding of public trust in their ability to manage future health crises in these institutions is needed.

A retrospective review of errors made during the pandemic can identify areas for improvement in the current healthcare system. Lack of preparedness, inadequate resources and insufficient capacity were highlighted in the pandemic. Resilience and capacity need to be planned for pandemic preparedness by investing in infrastructure, investing in research and development, and developing effective communication strategies.

## What we Could have Learned from the 1918 Spanish Flu (H1N1) Pandemic

In the early twentieth century, the H1N1 virus, the Spanish Flu, saw one of the deadliest pandemics in human history. It is estimated that 500 million people across the globe were infected, and at least 10% of them (50 million) died. The

first lesson we could have taken was the successes seen in early detection and quick interventions. In a study comparing the response time and outcomes from two United States cities, Philadelphia and St. Louis, the stark difference in rapidity to response is clear (Markel *et al.* 2007).

Philadelphia hosted a parade during the early days of the Spanish Flu pandemic; within days, hospitals were at capacity, and 2,600 people had died. Concurrently, two days after the first case of Spanish Flu was noted there, St. Louis imposed strict lockdown measures, including closing schools and public gathering places. Passenger number limits on public transport were imposed, and work shifts were staggered to minimise contact. Philadelphia eventually imposed the same measures two weeks after their first cases were reported. The differences in time to decisive action between these two cities led to vastly different outcomes. From September 1918 to February 1919, the northern hemisphere winter, the death rate was approximately 358 per 100,000 in St. Louis and 748 per 100,000 in Philadelphia (Markel *et al.* 2007)

A reflection on the COVID-19 pandemic will likely show similar outcomes, although a one-size-fits-all strategy does not work, as will be demonstrated later. The WHO took months to declare the pandemic, resulting in countries where infections began in January to March 2020, such as Italy (with an older population), having poor outcomes, while countries receiving their first cases after March 2020, when the WHO declared the pandemic, were not as severely affected. The WHO's tardy response led to initial poor outcomes in countries with early infections. The final verdict appears to be damning according to the studies by Steve Hanke and co-workers (Herby 2023).

Brooks Hospital near Boston in Massachusetts implemented a novel approach to treatment for the Spanish flu based on their experience as a TB hospital. They implemented open-air treatment, which proved successful in reducing mortality (Hobday & Cason 2009). Patients were treated in tents outside the hospital, where they had access to fresh air and sunlight, as opposed to the traditional medical practice of keeping patients in closed, cramped wards. The maximum ventilation provided by the outdoor space reduced airborne transmission, and the sunlight would have impacted improved Vit D in the patients. These practices that were shown to be successful in the Spanish Flu pandemic in a single hospital were ignored during the COVID-19 pandemic, where patients were primarily isolated in wards without natural light. While open-air treatment is not always feasible, good ventilation and vitamin D benefits could have been acknowledged early in the pandemic.

## Indiscriminate Lockdowns

The implementation of lockdowns as a preventative measure in controlling the spread of infectious diseases has been a topic of considerable discussion, dating back to the success witnessed in St. Louis during the 1918 pandemic. Indeed, the onset of the COVID-19 pandemic brought this strategy to the forefront once more with the initiation of lockdowns in Wuhan, China, where the virus was first detected, a methodology subsequently adopted globally in varying degrees. Early adoption of lockdowns appeared to be a key determinant in effectively managing community transmission. This strategy showed a higher success rate than Italy's approach, which initiated lockdowns following the WHO's official pandemic declaration (Khanna *et al.* 2020). While numerous studies affirm the efficacy of lockdowns in curbing the spread of the virus (Caristia *et al.* 2020; Juul *et al.* 2022), there remains a substantive discourse advocating for a more nuanced approach to their implementation, suggesting a tailored strategy that considers various factors to be more prudent (Hu *et al.* 2021; Zhou, Zhang & Qu 2020).

However, a contrasting perspective posits that lockdowns may not be the most effective strategy, particularly in managing airborne diseases, arguing for exploring alternative approaches to control community transmission (Herby. J 2023; Herby 2022) This divergence in opinions among the scientific community underscores the complexity of managing pandemics. A recent study found that mass gatherings during COVID-19 did not increase the spread of the virus (Feltham *et al.* 2023). It raises pertinent questions on the optimal strategies to adopt to mitigate such health crises' impacts.

As we delve deeper into this topic in the subsequent sections, we aim to propose a strategy that navigates these complex challenges effectively, drawing upon the lessons learned from the multifaceted responses to COVID-19. The goal is to foster a balanced approach that leverages the strengths of lockdowns while mitigating their downsides, thereby promoting a response strategy that is effective, sustainable, and adaptable to the dynamic nature of pandemics. This would involve an in-depth exploration of various dimensions, including, but not limited to, the timing of implementation, the scale of lockdowns, and incorporating other preventive measures in a multifaceted approach to managing future pandemics. It remains imperative that future strategies are developed with a grounded understanding of the diverse perspectives and emerging evidence to foster resilient systems capable of protecting global health.

Hard lockdowns caused widespread economic disruption, including job losses, business closures, and decreased economic activity, which has resulted in financial distress for many individuals and businesses (Ozili 2020). However, measures that were proven successful in curbing transmission in sectors considered essential work, such as limited numbers of people in public transport and on the work floor, could be implemented more widely to allow more business to continue.

Lockdowns impacted considerably on mental health, leading to increased stress, anxiety, and depression for many people, particularly those who live alone or in residences away from their families. Lockdowns prevented older people from seeing their families, leading to compromised mental health. Open-air visits, such as those encouraged when visiting TB patients, would go a long way to ameliorating emotional stress in people living in homes for older or disabled people. The compromise based on known epidemiological interventions such as social distancing and fresh air would prevent hard lockdowns' most severe negative emotional impacts (López-Castro *et al.* 2021). The lockdowns disrupted education, leading to school closures and the transition to remote learning. This has resulted in decreased educational opportunities and increased disparities in access to education, particularly for low-income students and those without access to technology.

The lockdown strategy delayed medical care for many people, as hospitals and clinics focused on treating COVID-19 patients, and chronic patients did not feel they could get to health facilities to receive care. This has resulted in adverse health outcomes for some individuals unable to receive necessary medical care (Kapitsinis 2021). Addressing the continued chronic healthcare of individuals through a lockdown is a complex process involving possible online strategies for consultation and delivery of treatments to homes or central points.

The lockdowns helped mitigate the spread of SARS-COV-2. However, in retrospect, it is clear that lockdowns had significant social and economic impacts. A reflection on the level of lockdown in various contexts should be retrospectively analysed. For example, when a large part of the population is asymptomatic, it makes more sense to focus on measures to protect the vulnerable while the healthy group can continue with their work.

The lockdowns disrupted education, leading to school closures and the transition to remote learning. This has resulted in decreased educational opportunities and increased disparities in access to education, particularly for low-income students and those without access to technology (Onyema 2020).

The lockdown strategy delayed medical care for many people, as hospitals and clinics focused on treating COVID-19 patients, and chronic patients did not feel they could get to health facilities to receive care. This has resulted in adverse health outcomes for some individuals unable to receive necessary medical care (Kapitsinis 2021). Addressing the continued chronic healthcare of individuals through a lockdown is a complex process involving possible online strategies for consultation and delivery of treatments to homes or central points.

The lockdowns helped mitigate the spread of SARS-COV-2. However, in retrospect, it is clear that lockdowns had significant social and economic impacts. A reflection on the level of lockdown in various contexts should be retrospectively analysed. For example, when a large part of the population is asymptomatic, it makes more sense to focus on measures to protect the vulnerable while the healthy group can continue with their work.

## Cigarette and Alcohol Bans

As part of their responses to the COVID-19 pandemic, Thailand, India and South Africa implemented cigarette and alcohol bans (de Villiers, Cerbone & Van Zijl 2020). The rationale was weak, especially in light of the already-in-place lockdowns. It was anticipated that banning cigarettes and alcohol would limit social gatherings and promote public health. Smoking and drinking were believed to cause uninhibited social behaviour, resulting in non-compliance with physical social distancing practices meant to reduce transmission risk. Lockdown strategies already limited social gatherings, and banning cigarettes and alcohol, which are addictive, is less likely to reduce substance addiction than forcing the trade underground. The consequences of the bans have been complex and varied.

Several considerations influenced the decision to ban cigarette sales during the lockdown. One belief was that smoking might compromise the immune system, potentially increasing smokers' vulnerability to infections. In South Africa, Cooperative Governance Minister Dr Nkosazana Dlamini-Zuma, raised concerns regarding the communal sharing of cigarettes, which could potentially facilitate the transmission of the virus. This contentious prohibition sparked widespread discussion and inspired satirical commentary through pop culture. Max Hurrel from The Kiffness in South Africa leveraged the ban as a muse for a parody song, which quickly gained traction and went viral after being

uploaded on YouTube. Their song humorously explores the repercussions of the ban, providing a light-hearted take on a serious issue faced by the nation during the lockdown period (Hurrell 2020).

The loss of revenue to both businesses and the government was substantial due to these bans. These products contribute significantly to national economies, and the losses to governments regarding sin taxes, VAT, and other taxes were sizeable. With the supply of cigarettes and alcohol curtailed, a black market for these products emerged. Home-brewed, counterfeit and illegally imported and produced products became available. Health concerns arose around these black-market products' poor quality and potentially toxic effects. Authorities ignored health issues around the sudden withdrawal of these substances. Withdrawal symptoms experienced by those dependent on cigarettes and alcohol experienced health problems and mental distress. There was no intervention to support people struggling with addiction during the pandemic.

An alternative strategy that could have been implemented would have decreased any adverse effects of alcohol or smoking during the COVID-19 pandemic. Education interventions to inform the public of the risks of smoking and drinking during the pandemic could have been implemented. Known health issues specific to the relationship between COVID-19 and substance use could have been highlighted to encourage the responsible use of these substances. Lockdowns and bans on social gatherings had already addressed many concerns about smoking and drinking as a conduit for virus transmission.

## The EBM Pyramid Model in mis-Understanding EBM

Evidence-based medicine (EBM) has been around for a while, but it wasn't until the 1990s that it became a major focus in medical education (Guyatt 1992). The idea behind EBM is that medical decisions should be based on science that has been peer-reviewed and tested rather than hunches or following trends. The essence of Evidence-Based Medicine (EBM) initially revolved around an informed assessment of all pertinent, peer-reviewed evidence across varying study designs to guide treatment recommendations and decisions. Fundamental to EBM was the ability to gauge the relative certainty of evidence derived from a particular study design, thereby leveraging the power to make informed inferences from gathered data. The Evidence-Based Medicine (EBM) foundation was built on the principle of integrating all accessible peer-reviewed evidence, irrespective of the research design, in formulating treatment recommendations and choices.

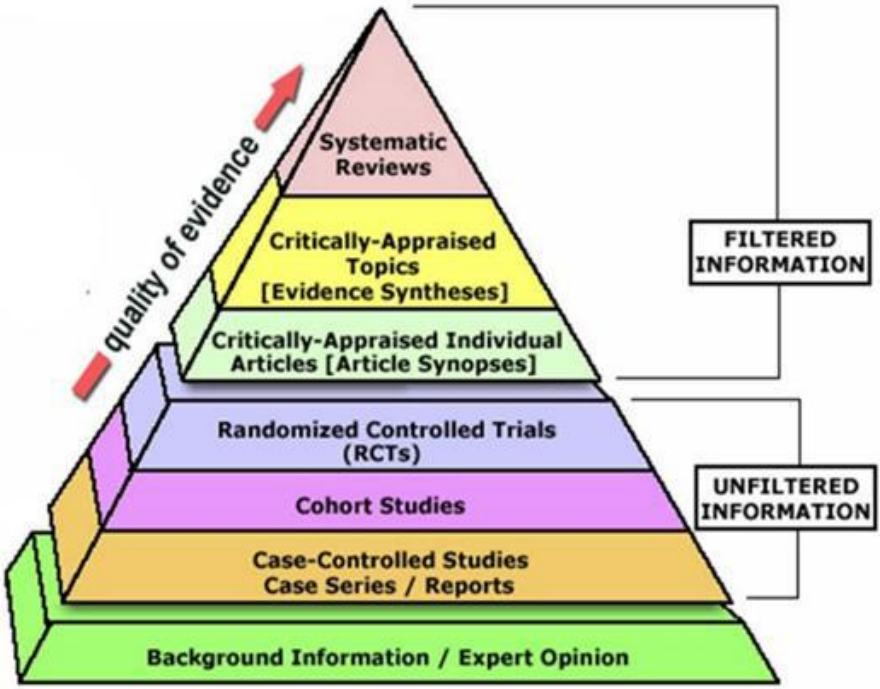



**Figure 1.** The traditional evidence-based medicine Pyramid model represents a purported hierarchy of ever-increasing quality. This Photo by Unknown Author is licensed under CC BY-SA-NC (UF 2024).

Unfortunately, in recent years, EBM has been misunderstood and misapplied due to the emphasis on a hierarchy of evidence that ranks certain types of research as being of higher quality than others. This has led to valuable data and treatment options being overlooked.

As outlined in the illustrative EBM pyramid model (Figure 1), the transition towards a hierarchical representation of evidence quality instead of certainty levels marked a pivotal shift in EBM's interpretative and application landscape. This paradigmatic shift inadvertently relegated Real-World Evidence (RWE) and other lower certainty reports to a peripheral role, with a preference for randomised controlled trials (RCTs) and meta-analyses thereof dominating the clinical and governmental decision-making echelons. It negates

the potential insights that could be harvested from high-quality case-controlled studies and overlooks the pitfalls of poorly executed double-blinded RCTs (DBRCTs).

Regrettably, the prevailing EBM pyramid, embodying quality labels, has fostered a rigid perspective, emphasising RCTs as the gold standard while undermining the contribution of RWE, thus compromising the utilisation of repurposed drugs notwithstanding their established safety profiles. This stance, echoed in medical pedagogy and media narratives, not only disenfranchises the merits of RWE but also inadvertently endorses flawed RCTs, a phenomenon underscored by the critical evaluation of widely cited RCTs referencing ivermectin's efficacy in COVID-19 treatment. The widely accepted yet misguided practice of conflating quality with certainty and featuring a 'quality' label on the pyramid in Figure 2 has ingrained the notion that only RCTs and their meta-analyses should be considered for most clinical and governmental decision-making. This stubborn insistence on RCTs for repurposed drugs with a well-established safety profile, without considering the totality of evidence, including RWE, has frequently led to overlooking or delaying the implementation of effective treatments.

Furthermore, medical education and media narratives have ingrained the belief in frontline medical professionals and the general public that, by default, RWE is of inferior quality and RCTs are of superior quality. As expressed in a medical school textbook: '*If the study was not randomised, we would suggest that you stop reading it and go on to the next article*' (Strauss *et al.* 2018). Poorly constructed or executed RCTs have been accepted as high quality, not because of their actual scientific merit, but due to their position in the pyramid model. The most widely publicised RCTs used to justify governmental policies regarding the ineffectiveness of IVM for treating COVID-19 have exhibited flaws in design or scientific integrity.

A re-evaluation of the prevailing EBM approach is needed, recognising that observational studies can, in certain contexts, resonate with the findings from well-conducted RCTs, thereby facilitating early treatment strategies informed by initial case studies. Hence, it is prudent to acknowledge the value of preliminary studies in steering research and treatment trajectories.

## Evidence-based Medicine in a Pandemic

Aldous *et al.* introduced the Totality of EBM (T-EBM) Wheel (Aldous *et al.* 2024) which takes a different approach to evaluating research. Instead of using

a hierarchy of evidence, the T-EBM Wheel includes all types of research, both peer-reviewed and real-world evidence (RWE), and visualises them in a colour-coded format. This allows for a more comprehensive understanding of the totality of evidence available.

During a pandemic, the need for RWE is critical, as it can provide valuable information about the efficacy of treatments before randomised controlled trials (RCTs) are available. This is especially relevant for repurposing drugs already known to be safe. Our article provides a proof of concept by constructing a T-EBM Wheel for the efficacy of treating COVID-19 with IVM-based regimens.

By rethinking how we evaluate evidence in medicine, we can ensure that all types of research are considered and that valuable treatments are not overlooked during times of crisis.

## The Totality of Evidence Wheel

The advent of the Totality of Evidence-Based Medicine (T-EBM) wheel presents a revitalised framework, accommodating a broader spectrum of reports encompassing those found in the traditional EBM pyramid. With the integration of an outer ring delineating various outcomes and facilitating a visual representation of report volumes, this innovative model fosters a comprehensive overview. Furthermore, the colour-coded segmentation within the outer ring enables a discernible representation of potential clinical equipoise instances, enhancing diagnostic visualisation.

The T-EBM wheel emerges as a versatile tool to guide medical professionals and policymakers, encapsulating a rich dataset devoid of the misleading quality-certainty hierarchical delineation inherent in the pyramid model.

Consequently, this progressive tool is primed to evolve into a pivotal application tool, relegating the pyramid model to a pedagogical role, elucidating evidence certainty, and spearheading a transformative approach in evidence-based medical practice rooted in a holistic, inclusive, and nuanced assessment of available evidence. It is imperative, moving forward, to adopt such comprehensive models to ensure that the breadth of the available evidence is considered in both clinical settings and policy formulation, fostering outcomes that are robust, inclusive, and truly representative of the collective evidence at hand.

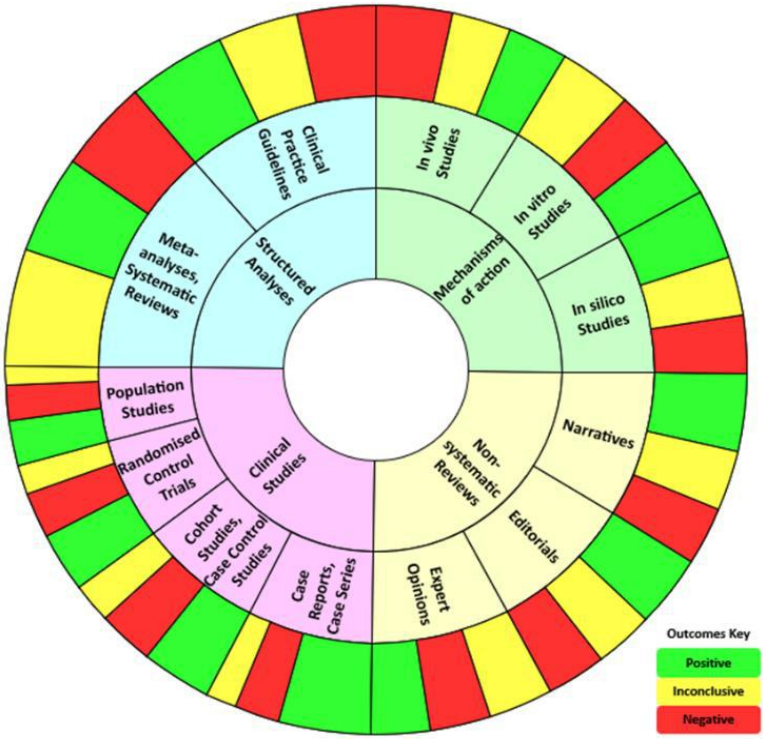



**Figure 2.** Totality of Evidence-Based Medicine (T-EBM) Wheel for peer-reviewed research. The inner ring of the wheel catalogues reports by four types: mechanisms of action and clinical studies, which are sources of primary evidence, and structured analyses of primary data and reviews, which are the secondary reports based on the primary evidence. Each inner ring section is disaggregated into one or more middle ring sections with the same coloring. In turn, each middle ring section is disaggregated into three outer ring sections by the outcomes of its reports, namely: 'positive', 'inconclusive', 'negative'. The legend in the lower right-hand corner of the figure shows the color-coding for each of the outcomes. The size of each section of a ring will be proportional to the number of reports in the literature for that section. The Excel Sunburst used to create the wheel orders each section in the inner ring clockwise from largest to smallest. As one moves outward from the inner ring, the subsections of a given section are similarly ordered clockwise from largest to smallest (Aldous *et al.* 2024).

The T-EBM wheel, a model that encapsulates a broader spectrum of evidence inclusive of a proportional representation of diverse outcomes, offers a more holistic approach towards understanding the dynamics of efficacy and safety in medical scenarios, enhancing the strategic approach employed by clinicians and decision-makers. Figure 3 shows that the Wheel includes everything the pyramid does and more.

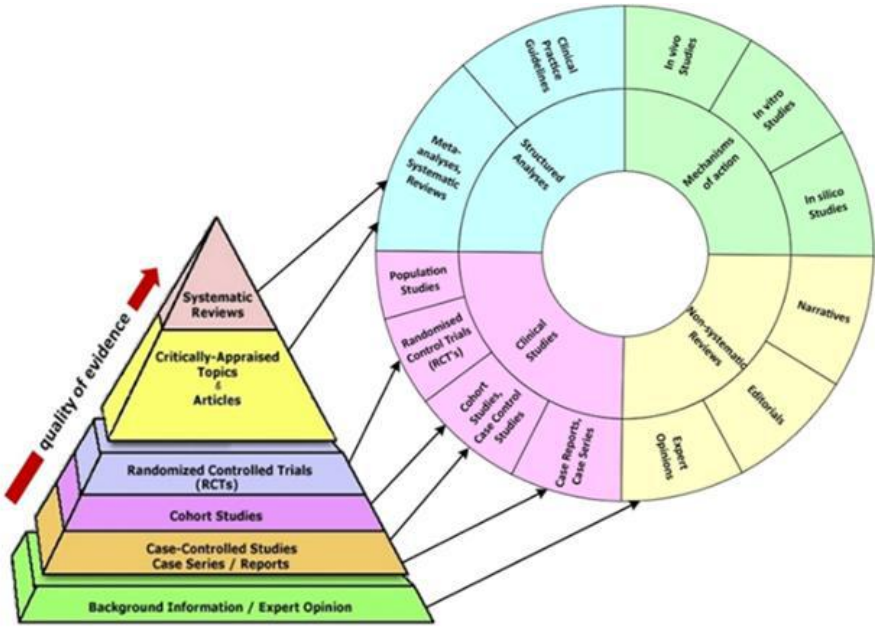



**Figure 3.** Correspondence of traditional EBM Pyramid with the middle ring of T-EBM wheel. Arrows show correspondence between levels of the pyramid and sections of the middle ring of the T-EBM wheel. The inner ring is included to show how middle ring sections arise from partitions of inner ring sections (indicated by colour coding).

The T-EBM wheel enriches medical decision-making by integrating an array of evidence types focused on distinct outcomes, thereby establishing a comprehensive foundation that supports the amalgamation of Real-World Evidence

(RWE) and not excluding Randomized Controlled Trials (RCTs). This synergy guides medical professionals in crafting individualised treatment strategies while evolving a communal standard of care, nurturing a cohesive strategy bolstered by a comprehensive evidence base. Notably, while a single observational study may carry less certainty than a single RCT, studies of the same disease should yield similar results, regardless of whether the studies are observational or RCTs. Only case studies are available during the early stages of a disease outbreak, with no RCTs. Therefore, it is likely that the results of successful earlier case studies will align more with those from successful RCTs conducted later. Therefore, it is crucial to utilise the indications from these early studies to guide treatment and further research.

## Utility of the TEBM Wheel

In the critical early stages of a pandemic, the T-EBM wheel model could have proposed a versatile approach to treatment strategies, suggesting a potential departure from the often resource-intensive and slow process of initiating double-blinded RCTs. This model advocates for the immediate exploration of repurposing existing medications grounded in the retrospective analysis of diseases bearing analogous traits.

The T-EBM wheel enhances the representation of various types of evidence, going beyond the features included in the traditional EBM pyramid, as illustrated in Figure 1. This expansion is visually depicted through an added outer ring in the complete wheel, offering insight into different outcome types and facilitating a clearer perception of the relative volume of diverse reports. By adopting a colour-coded system in the outer ring, as highlighted in Figure 2, practitioners can more readily identify instances of clinical equipoise. Contrasting the pyramid model, which primarily serves educational purposes by teaching evidence certainty, the wheel disregards the potentially misleading quality/certainty hierarchy present in the pyramid, promoting itself as a superior tool for practitioners and decision-makers to implement in the medical field.

In this agile paradigm, the initial focus is leveraging studies conducted *in vitro, in vivo,* and *in silico* to rapidly identify early markers of efficacy, promoting a proactive posture in treatment interventions. While acknowledging the possibility of Type 1 errors emerging from these exploratory drug protocols, the model contends that such risks remain controllable, especially when founded on well-strategised dosing plans.

Furthermore, the model underscores the critical role of frontline healthcare professionals, encouraging the assimilation of their first-hand clinical insights into the decision-making vortex. Such ground-level Intelligence, combined with observational studies and case analyses, promises to shape potent clinical protocols for ensuing RCTs, nurturing a responsive and adaptive blueprint for treatment.

This approach warrants a dynamic monitoring framework wherein governmental and medical establishments continually scrutinise the evolving results, steering expansive experimental implementations judiciously. It is envisaged as a living tool, necessitating regular updates to encapsulate the dynamic landscape of evidence surrounding treatment methodologies, empowering stakeholders to stay receptive to positive indications and steering research and announcements through a real-time evidence canvas.

Enabling an informed practice of off-label drug utilisation demands an in-depth exploration of existing literature, ensuring comprehension of safety profiles and possible efficacies. It cultivates a culture that thrives on data-rich resources, enabling healthcare practitioners to execute interventions grounded in robust evidence. It fosters a future where the enlightened and adaptable deployment of entrenched and emerging evidence steers healthcare.

The T-EBM wheel echoes the principles seen in the circular social sciences model, offering a repository of a wide variety of evidence and presenting a proportional portrayal of outcomes, albeit limited to individual results types such as safety or efficacy. The T-EBM wheel envisions guiding clinicians and decision-makers through a rich array of information essential in harmonising RCTs with real-world evidence (RWE). It distinctly facilitates the integration of the complete evidence spectrum, aiding medical professionals at the forefront to weave RWE and available RCTs with their observations, fostering a ‘community standard of care’.

The design and upkeep of the T-EBM wheel mandate its periodic update to present a timely visualisation of the evolving gamut of evidence on treatment protocols. This tool, serving as a visual compass, systematically organises a myriad of evidence in an accessible, intuitive manner, encouraging an approach eschewing biases birthed from misapplying the pyramid model.

Guided by the earnest goal of collating timely and actionable data, the approach insists on meticulous scrutiny, balancing high internal validity methodologies like placebo-controlled RCTs with extensive, long-term observational studies that document real-world clinical practice implications. It persuades a departure from an over-reliance on randomised studies, urging the

adoption of techniques optimised to answer pertinent questions with the utmost scientific rigour.

Thus, this approach not only signals a shift in the strategic execution of pandemic responses but also paves the way for a future where evidence-based medical strategies are characterised by adaptability, inclusivity, and forward-thinking, armed with a continuously evolving repository of actionable data drawn transparently and objectively from a wider spectrum of evidence. It nurtures a culture guided by the dictum, 'Here's what we recommend and why,' steadfast in its pursuit of enlightened healthcare pathways grounded in comprehensive and adaptive utilisation of existing and emergent evidence.

Looking ahead, using the T-EBM wheel advocates for a more rounded approach to medical decision-making, urging medical practitioners and authorities to remain open to evolving evidence. It proposes a shift from the traditional hierarchical pyramid model of evidence evaluation to a tool that respects a spectrum of research outcomes. This would ideally foster a community standard of care that integrates various pieces of evidence and real-world observations to navigate treatment strategies effectively.

Moreover, it suggests that during pandemics, medical professionals should have the flexibility to experiment with repurposed drugs known to be safe. This could potentially aid in finding effective early treatments and prevention strategies, potentially attenuating the impacts of pandemics like COVID-19.

## The TEBM Wheel Assessment of Ivermectin

The use of ivermectin (IVM) as a therapeutic agent in the COVID-19 pandemic has been controversial. Before the pandemic, IVM had a well-established safety record, confirmed by the World Health Organization's VigiAccess database. Despite some studies showcasing the potential benefits of IVM, the global scientific community has not reached a consensus regarding its efficacy in treating COVID-19. This is partly due to active press and social media campaigns against its use and conflicting results from various studies, some of which have been criticised for poor design and execution.

To clarify this topic, an independent actuary was asked to conduct a comprehensive search for published reports on PubMed to analyse the evidence available for IVM's use in COVID-19 treatment since 2020.

The analysis focused on 265 studies, exploring their findings, which

ranged from positive and negative to inconclusive outcomes.

Aldous *et al.* (2024) introduced the T-EBM wheel tool to visually represent the totality of evidence from various studies, emphasising a non-hierarchical approach to evaluating research findings. This tool aims to foster a comprehensive and unbiased view of the existing research, highlighting the necessity to consider broader evidence rather than relying solely on randomised controlled trials (RCTs). The 265 studies were represented in a TEBM-Wheel for ivermectin, see Figure 4.

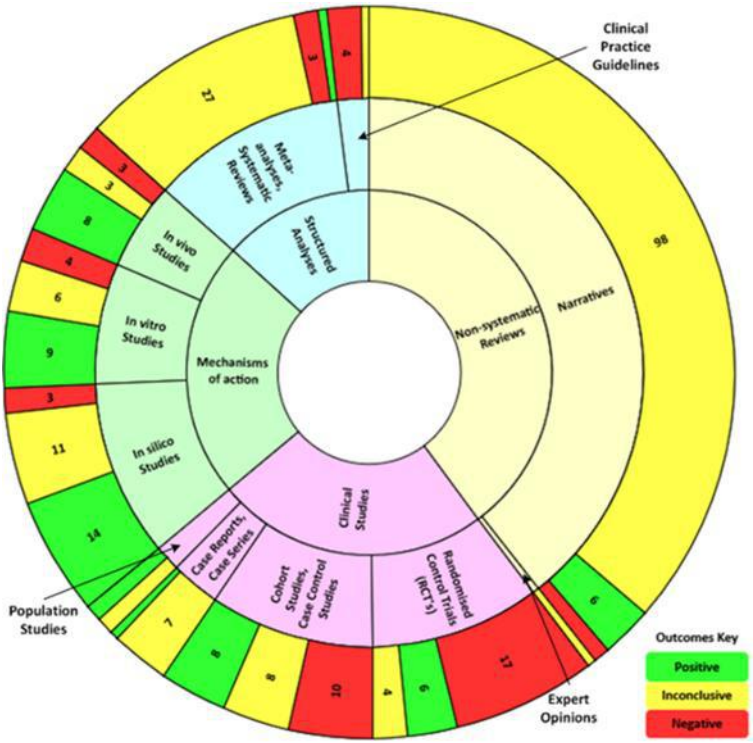



**Figure 4.** IVM T-EBM wheel for the efficacy of IVM-based regimens treating COVID-19 (IVM Wheel). Data from peer-reviewed published reports listed in Pubmed and searched for 'ivermectin' and for 'COVID-19' or 'SARS'. The number displayed in each outer ring section is the number of its reports.

A closer look at the data revealed that protocols with more successful outcomes tended to involve higher dosages of IVM, combination therapies, and longer treatment regimens. However, the effectiveness of IVM-based treatments remains unclear, warranting further research to ascertain its potential benefits and drawbacks in treating COVID-19.

In conclusion, while the findings regarding IVM's efficacy are mixed, the T-EBM wheel presents a promising approach to facilitate a more nuanced understanding and assessment of treatment strategies, calling for a cooperative and informed approach to tackling pandemics in the future.

## Holistic Management of Pandemics (Aldous & Kruger 2023)

The COVID-19 pandemic has revealed many flaws in decision-making processes and policies, one of which is the lack of diversity among decision–makers. Globally, COVID-19 pandemic responses were led by a few select individuals, mainly clinicians. They lacked diversity in their backgrounds and perspectives as individuals and as a group. They led the initial responses and were supported by government officials. There were no social scientists, economists, legal specialists or pure scientists contributing thought that would impact mental health, the economy, conflicts of interest and human rights, or evidence-based medicine. With the same backgrounds and perspectives, this select group had blind spots in decision-making and policy development and overlooked important considerations critical to a successful response. A limited range of solutions and strategies were developed in lock-step globally, ignoring creative or innovative approaches to managing the pandemic from other discipline thinkers. There was a failure to address the broader societal impacts of the pandemic.

The leadership by politicians and public health scientists led to a narrow focus on specific aspects of the pandemic response. Policies and strategies did not consider the needs and experiences of diverse communities, the economy or broader human rights. Initial reactions focused on novel medical interventions such as testing and vaccine development while neglecting the social and economic impacts of the pandemic. Many low-income communities had limited access to healthcare and were thus disproportionately affected by the pandemic because the decision-makers did not understand their unique challenges. As more general hardships became apparent and 'facts' initially presented as certain were changed or proven wrong, a lack of trust and confidence in the response led almost exclusively by clinically trained people developed.

Washing hands, social distancing and staying home were early messages about preventing COVID-19 transmission. This did not consider the circumstances of shack dwellers who have limited access to water and live in single-room accommodations that are often uninhabitable during the day because of the building materials used.

In over four decades, Alan Savory has devised and implemented Holistic Management principles in agricultural and grassland conservation sectors globally, promoting a balance of economic, social, and environmental factors (Institute 2023; Savory & Butterfield 1999; Savory & Butterfield 2016). During the onset of the COVID-19 pandemic, the notion of extending these principles (Gosnell *et al.* 2020) to manage future pandemics began to crystallise, encouraging a comprehensive solution incorporating various critical dimensions.

An exploration into existing literature unveils the gradual incorporation of holistic viewpoints in various domains, such as economics (Ponte *et al.* 2016) health (Constantinou *et al.* 2020; Fardet and Rock 2014; Wang and Teo 2021) marine management (Rodriguez 2017), biology (Mazzocchi 2012), and environmental management (Barrera 2020; Seminara & Bolla Pittaluga 2012; Younos, Lee & Parece 2018) shifting away from the previously favoured reductionist models, which faced criticism for their limited perspective (Andersen 2001; Ribatti 2021).

Interestingly, it required a military leader (General Stanley McChrystal) to realize that reductionist management style is no longer feasible in modern organizations within a networked world, working with complex systems and where small changes can create non-linear and non-predictable reactions/ outcomes (McChrystal 2015). According to McChrystal, modern organizations require Gardeners (facilitators/ enablers) rather than Chess masters (centralized decisions) as leaders. Gardeners nurture the environment in which all the pieces (the other team members) can thrive. This require sharing of information and devolution of decisions as far as possible.

With this background in mind, it is quite clear that perhaps the biggest mistake of Governments dealing with the COVID-19 pandemic, was to centralize decisions around mostly one Pandem-Icon (Joubert *et al.* 2023) Scientists. The result was that a reductionist approach was followed to break down a complicated problem [with social, economic and environmental (health, the virus) factors] into linear, deterministic and measurable relationships. In the process they found/proposed a simplified solution (hard lockdowns and a new RNA based vaccine), ignoring all other equally important factors. Any alternative treatment was also vilified.

The world-wide lack of diverse and multidisciplinary COVID-19 advisory panels resulted in a typical reductionist solution at a huge cost in terms of economic, social and the health environment:

In terms of the effect of reductionist pandemic management on social aspects, (Bhattacharya, Smark & Mir 2021; Caro *et al.* 2022; Kamath *et al.* 2022; Mahagamage & Marasinghe 2023; Rainer *et al.* 2022) it is clear that the result was devastating. Despite many reports on increased suicides (Cozzi *et al.* 2023; Ogrodniczuk *et al.* 2023; Wasserman *et al.* 2020) there was no significant increase (in most countries) during the pandemic (Appleby 2021; Cozzi *et al.* 2023; Ogrodniczuk *et al.* 2023; Pirkis, Gunnell, Shin, Del Pozo-Banos, Arya, Aguilar 2022; Pirkis *et al.* 2021; Wasserman *et al.* 2020). However, ongoing economic hardship and suffering may lead to increased suicide cases in future.

Finally, the reductionist management model from the Pandem-Icons also got it wrong in terms of the health environment. Locking people up and not allowing them to go outside, turned out to be disastrous, especially for the elderly in Nursery Care Homes in the USA (Chidambaram 2022).

One can understand the initial panic when the pandemic broke out in December 2019. The fact that it started in China, who seemed to have limited free flow of information, did not help. The initial world-wide response by most Governments was responsible. However, they should have known better quite early on.

A cruise ship (the Diamond Princess) experienced a major outbreak on board and it was quarantined in Japan (Yokohama) on 4 February 2020 for about a month (Smiley 2020) From the 3711 passengers and crew, around 700 people became infected and 9 people died. This was a 'God-given' scientific experiment that showed early on that more than 80% of people appears to be asymptomatic to the virus. Although scientists concluded in July 2020 that the COVID-19 virus is airborne (Morawska & Milton 2020) it took much longer for the WHO and CDC to admit it. So, within about 6 months, it was known that ALL passengers and crew on the Diamond Princess were exposed to this airborne virus, and less than 20% were susceptible to it. Later reports confirmed that about 85% of people are asymptomatic towards the virus (Hao *et al.* 2020; Lei *et al.* 2021).

In addition to that, it was also known quite early during the pandemic (from deaths in Italy) (Minnai *et al.* 2022), that most deaths were people above 65 years of age. The importance of co-morbidities (Russell, Lone & Baillie 2023) was also known, relatively early on during the pandemic.

In hindsight it seems quite possible that a diverse and multidisciplinary COVID-19 advisory panel practicing Holistic Management principles would have recommended maximum protection of the elderly and vulnerable, rather than a hard-lockdown strategy. Ironically, even though South Africa was applauded for one of the strictest lockdowns apart from China (Campbell 2020) we are the country with most possibly the highest infection rate (98%) in the world (already by March 2022) (Bingham 2022). There is a simple explanation for this: the majority of the South African population (working in our shops, hospitals and homes) uses minibus taxis for commuting on a daily basis. As early as June 2020, the taxi industry rejected the South African government's strict travel restrictions (Reuters 2020). The result was that the virus spreaded uncontrolled *via* these heavily loaded taxis. This failed experiment confirms our point that a 'one size fits all' strategy did not work for COVID-19.

Social science, economic and legal insights into pandemic preparedness, and public health insights would lead to a pandemic response that could prevent the financial disaster of the COVID-19 pandemic and alleviate the mental well-being issues it brought about. Leadership positions in future pandemic responses should prioritise diversity of thought. This should include actively seeking diverse perspectives and experiences to ensure diverse voices are represented in decision-making processes. This will ensure that strategies are inclusive and well thought through, leading to a more effective and equitable response. Strategies would include improved health communication tailored to diverse communities needs, and workplace safety for all workers could be designed so that lockdowns would not require the shutdown of all industries.

Including social scientists, legal experts, and economists in a pandemic response team is essential because pandemics are not just a medical problem but also a social, legal, and economic issues. While clinically trained people and politicians can provide necessary expertise, they may not have the same level of knowledge or understanding regarding the broader social, legal, and economic impacts of a pandemic.

Social scientists can bring their expertise in understanding human behaviour, social dynamics, and cultural factors that can influence disease spread and interventions' effectiveness. They can also help identify and address potential social and behavioural barriers to adherence to public health measures, such as vaccine hesitancy or resistance.

Legal experts can guide the legal frameworks and policies necessary for a coordinated response to a pandemic, such as emergency powers and

quarantine measures. They can also help ensure that public health interventions are implemented in a way that respects individual rights and liberties.

Economists can help assess the economic impact of a pandemic and the measures taken to address it, such as lockdowns or business closures. They can also provide recommendations on mitigating economic damage, supporting affected industries and workers, and ensuring that the pandemic response is equitable and sustainable.

Scientists who are not clinicians are essential members of a pandemic response team because they provide the foundational knowledge necessary to understand the biology and behaviour of the virus. While clinical and medical scientists focus on developing treatments and vaccines, pure scientists study the virus's underlying mechanisms, help identify potential drug targets, and can look at evidence-based medicine more holistically.

Pure scientists can conduct experiments and analyse data to understand how the virus spreads, mutates, and interacts with host cells. This knowledge can inform public health policies and control measures, such as social distancing guidelines and vaccination strategies. Additionally, pure scientists can help identify potential weaknesses in the virus that can be exploited to develop effective treatments and vaccines.

Without the contributions of pure scientists, clinical and medical scientists are limited in their ability to develop effective treatments and vaccines. Pure scientists provide the necessary knowledge and understanding of the virus, enabling clinical and medical scientists to develop targeted interventions.

A pandemic response team must have diverse discipline thinkers with different specialisations (Finance, Health, Humanities, Legal etc.). By working together, these scientists can provide a more comprehensive understanding of the virus, leading to more effective interventions and control measures. A pandemic response team that includes a diverse range of experts can provide a more comprehensive and effective response to the challenges posed by a pandemic.

In contrast, Sweden's management of the pandemic, which demonstrated a more balanced approach prioritising not only health but also economic and social factors, showcases the potential merits of a holistic strategy, presenting a model with reduced excess deaths compared to several other nations (Britschgi 2023; Norberg 2023; Andersson & Jonung 2024).

Time will teach us to what extent the shocking revelations by Dr David Martin about the origin and handling of the COVID-19 pandemic are true

(Martin 2022). Given the fact that most of the initial COVID-19 'conspiracies' turned out to be true, he is likely to be on the right side of history.

Conclusion:

As the international community continues to navigate the complexities of the COVID-19 pandemic, a pressing concern has emerged regarding the legal immunities bestowed upon vaccine manufacturers by governments globally and significant entities such as the WHO (Lintern 2020; Sigalos 2020; Wood 2020). These immunities present a pivotal issue, potentially encouraging expedited processes at the expense of rigorous safety assessments. The crux remains: Does the absence of legal accountability foster an environment where shortcuts are more feasible? It is a question demanding urgent scrutiny and comprehensive dialogue across various sectors of society.

Restoring their independence is essential to bolster the integrity of global health organisations like the WHO, FDA, and ECDC. We urge a concerted effort to re-establish these entities as bastions of unbiased, evidence-backed decision-making insulated from potential conflicts of interest. Implementing Independent Review Boards (IRBs) is a promising proposition, envisioned to oversee the safety protocols of new vaccine developments meticulously, ensuring transparency that reinforces public trust.

As the discourse evolves, it becomes increasingly apparent that there is a need for a profound reflection and deliberation on the extent of governmental influence during pandemic epochs. Societies globally are encouraged to actively engage in discussions delineating the confines of governmental power, fostering a collaborative effort to forge a pathway characterised by informed choices, securing our civil liberties and our collective well-being.

In line with this, we advocate instituting multidisciplinary pandemic advisory panels grounded in Holistic Management principles, characterised by a holistic overview encompassing various perspectives, thus steering away from reductionist approaches that may overlook significant factors. The integration of the 'Totality of Evidence-Based Medicine (T-EBM) Wheel' approach emerges as a seminal concept in this framework, seeking to cultivate a rich, nuanced perspective by considering a more comprehensive array of evidence, thereby forging strategies that are both responsive and inclusive (Aldous *et al*. 2024).

As we forge ahead in these unprecedented times, it becomes incumbent upon societies worldwide to foster environments where robust debates can thrive, encouraging a collective responsibility towards informed governance. Through enhanced transparency and collaboration, we must build a future

where responses to pandemics are grounded in holistic insights, evidential integrity, and the shared goal of global well-being. This strategy underscores a commitment to nurturing a landscape where decisions are responsive and framed with a deep-seated commitment to safeguarding the holistic health of communities globally. It is a call to arms for a more united, informed, and resilient world, ready to face the challenges of tomorrow with a spirit of unity and evidence-backed preparedness.

In unity and with hope, we look forward to a future where our collective efforts ensure the health and well-being of all, while maintaining a judicious balance of power, and ensuring just compensation for those affected by vaccine-related adverse events.

## References

Agresti, J.D. 2022. The Most Objective Evidence Shows No Indication that COVID Vaccines Save More Lives than they Take – *Just Facts Daily*. https://www.justfactsdaily.com/most-objective-evidence-covid-vaccines-lives

Aldous, C., B.M. Dancis, J.Dancis & P.R. Oldfield 2024. Wheel Replacing Pyramid: Better Paradigm Representing Totality of Evidence-Based Medicine. *Annals of Global Health* 90,1: 15. https://doi. org/10. 5334/aogh. 4341 <Go to ISI>://WOS:001226250700014. PMid:38435471 PMCid:PMC10906340

Aldous, C. & H.G. Kruger 2023. Interrogating the Lack of Diversity of Thought in the Pandemic Response that Led to Mistakes – Holistic Evidence-based Approach to Deal with Future Pandemics. *Frontiers in Public Health* 11: 1310210. https://doi. org/10. 3389/fpubh. 2023. 1310210. https://www. ncbi. nlm. nih. gov/pubmed/38192553 PMid:38192553 PMCid:PMC10771982

Andersen, H. 2001. The History of Reductionism versus Holistic Approaches to Scientific Research. *Endeavour* 25,4: 153 - 156. https://doi. org/10. 1016/s0160-9327(00)01387-9 <Go to ISI>://WOS:000173191400004.

Andersson, F.N.G. & L. Jonung 2024. The COVID-19 Lesson from Sweden: Don't lock Down. *Economic Affairs* 44,1: 3 - 16. https://doi. org/10. 1111/ecaf. 12611

Appleby, L. 2021. What has Been the Effect of COVID-19 on Suicide Rates? *BMJ* 372: n834. https://doi. org/10. 1136/bmj. n834 https://www. ncbi. nlm. nih. gov/pubmed/33782026 PMid:33782026

Apuzzo, M. & S. Gebrekidan 2021. Governments Sign Secret Vaccine Deals. Here's What they Hide. *The New York Times*. (Accessed in August 2024.) https://www. nytimes. com/2021/01/28/world/europe/vaccine-secret-contracts-prices. html.

Barrera, J.F. 2020. Holistic Pest Management; Book Chapter, Area-Wide Management of Fruit Fly Pests. <Go to ISI>://WOS:000530362400021.

Bassyouni, M. 2024. Opinion: 'I'm a vaccine scientist'. The Devastating Impacts of Vaccine Hesitancy have Touched my Life too. CNN Opinion (Accessed in Aug 2023.) https://edition. cnn. com/2024/08/06/opinions/vaccine-hesitancy-measles-health-bassyouni/index. html.

Bhattacharya, J. 2023. The Government Censored Me and Other Scientists. We Fought Back – and Won. | The Free Press. https://www.thefp.com/p/i-fought-government-censorship-and-won

Bhattacharya, S., C. Smark & M. Mir 2021. COVID-19: Social, Financial and Economic Implications. *Australasian Accounting Business and Finance Journal* 15,1: 1 - 4. https://doi. org/10. 14453/aabfj. v15i1. 1 <Go to ISI>://WOS:000613712000001.

Bingham, J., R. Cable & C. Coleman 2022. Estimates of Prevalence of Anti-SARS-CoV-2 Antibodies among Blood Donors in South Africa in March 2022. Europe PMC. Last Modified 5 (Accessed in August 2024.) https://europepmc. org/article/PPR/PPR498407. https://doi. org/10. 21203/rs. 3. rs-1687679/v1

Britschgi, C. 2023. Study: Sweden's 'Laissez Faire' Pandemic Policies Paid Off. Reason.com (Accessed in August 2024.) https://reason. com/2023/08/29/study-swedens-laissez-faire-pandemic-policies-paid-off/.

Bryant, A., T.A. Lawrie, T. Dowswell, E.J. Fordham, S. Mitchell, S.R. Hill & T.C. Tham 2021. Ivermectin for Prevention and Treatment of COVID-19 Infection: A Systematic Review, Meta-analysis & Trial Sequential Analysis to Inform Clinical Guidelines. *American Journal of Therapeutics* 28,4: E434 - E460. https://doi. org/10. 1097/mjt. 0000000000001402. <Go to ISI>://WOS:000681356600007. PMid:34145166 PMCid:PMC8248252

Campbell, J. 2020. President Ramaphosa Leads Strong Response to COVID-19 in South Africa | Council on Foreign Relations (Accessed in August 2024.)

https://www.cfr.org/blog/president-ramaphosa-leads-strong-response-COVID-19-south-africa

Caristia, S., M. Ferranti, E. Skrami, E. Raffetti, D. Pierannunzio, R. Palladino, F. Carle, R. Saracci, C. Badaloni, F. Barone-Adesi, V. Belleudi, C. Ancona, M. De Sario, A. Faragalli, L. Ferrante, R. Gesuita, E. Lapucci, S. Vecchi & A.I.E. Working Grp Evaluation Effecti 2020. Effect of National and Local Lockdowns on the Control of the COVID-19 Pandemic: A Rapid Review. *Epidemiologia & Prevenzione* 44: 5 - 6: 60 - 68. https://doi. org/10. 19191/ep20. 5-6. S2. 104. <Go to ISI>://WOS:000608034700013.

Caro, J.C., A.E. Clark, C.D'Ambrosio & C. Vogele 2022. The Impact of COVID-19 Lockdown Stringency on Loneliness in Five European Countries. *Social Science & Medicine* 314: 10. https://doi. org/10. 1016/j. socscimed. 2022. 115492. <Go to ISI>://WOS:000903910300010. PMid:36343461 PMCid:PMC9617690

Chen, J.Y., Z.J. Cheng, R.K. Gong & J.L. Li 2022. Riding out the COVID-19 Storm: How Government Policies Affect SMEs in China. *China Economic Review* 75: 23. https://doi. org/10. 1016/j. chieco. 2022. 101831. <Go to ISI>://WOS:000830584400002. PMid:35821798 PMCid:PMC9264906

Chidambaram, P. 2022. Over 200 000 Residents and Staff in Long-Term Care Facilities Have Died From COVID-19. Kff. org (Accessed in August 2024.) https://www. kff. org/policy-watch/over-200000-residents-and-staff-in-long-term-care-facilities-have-died-from-COVID-19/.

Chongloi, H. 2022. Trial by Media: Evaluating the Role of Mainstream Media and Fact-checking Agencies during the COVID-19 Pandemic. *International Journal of Human Rights in Health Care* 11. https://doi. org/10. 1108/ijhrh-07-2022-0070. <Go to ISI>://WOS:000871460400001.

Christenson, J. 2023. CIA Tried to Pay off Analysts to Bury Findings that COVID Lab Leak was Likely: Whistleblower. *New York Post (*Accessed in August 2024.) https://nypost. com/2023/09/12/cia-tried-to-pay-off-analysts-to-bury-covid-lab-leak-findings-whistleblower/.

Constantinou, C., O. Kolokotroni, M.C. Mosquera, A. Heraclides, C. Demetriou, P. Karayiannis, A. Quattrocchi & A. Charalambous 2020. Developing a Holistic Contingency Plan: Challenges and Dilemmas for Cancer Patients during the COVID-19. *Cancer Medicine* 9,17: 6082-6092.

https://doi. org/10. 1002/cam4. 3271.
<Go to ISI>://WOS:000550405200001.
PMid:32687677 PMCid:PMC7405276

Cozzi, G., A. Grillone, E. Zuliani, M. Giangreco, C. Zanchi, G. Abbracciavento, E. Barbi & A. Amaddeo 2023. Suicide Attempts and Eating Disorders in Adolescents, the Mental Health Wave of the Second Year of the COVID-19 Pandemic: A Paediatric Emergency Department Perspective. *Frontiers in Pediatrics* 11: 7. https://doi. org/10. 3389/fped. 2023. 1078274 <Go to ISI>://WOS:000928590200001. PMid:36762280 PMCid:PMC9905671

Cruickshank, M. & R.Z. Shaban 2020. COVID-19: Lessons to be Learnt from a Once-in-a-century Global Pandemic. *Journal of Clinical Nursing* 29:21-22: 3901 - 3904. https://doi. org/10. 1111/jocn. 15365 <Go to ISI>://WOS:000541724100001. PMid:32498115 PMCid:PMC7301028

Darcy, O. 2022. Right-wing Media Pushed a Deworming Drug to Treat COVID-19 that the FDA Says is Unsafe for Humans. CNN Business. https://www.cnn.com/2021/08/23/media/right-wing-media-ivermectin/index.html

de Villiers, C., D. Cerbone & W. Van Zijl 2020. The South African Government's Response to COVID-19. *Journal of Public Budgeting Accounting & Financial Management* 32,5: 797 - 811. https://doi. org/10. 1108/jpbafm-07-2020-0120.
<Go to ISI>://WOS:000763670800006.

Deese, K. 2022. Judge Scraps 75-year FDA Timeline to Release Pfizer Vaccine Safety Data, Giving Agency Eight Months. *Washington Examiner*. https://www. washingtonexaminer. com/news/2381224/judge-scraps-75-year-fda-timeline-to-release-pfizer-vaccine-safety-data-giving-agency-eight-months/.

du Preez, H.N., J. Lin, G.E.M. Maguire, C. Aldous & H.G. Kruger 2024. COVID-19 Vaccine Adverse Events: Evaluating the Pathophysiology with an Emphasis on Sulfur Metabolism and Endotheliopathy. *European Journal of Clinical Investigation* e14296. https://doi.org/10.1111/eci14296
https://www.ncbi.nlm.nih.gov/pubmed/39118373 PMid:39118373

Ducharme, J. 2020. Why Ventilators May Not Be Working Well for COVID-19 Patients | *TIME*. Time.com (Accessed in August 2024.) https://time.com/5820556/ventilators-COVID-19/

Epstein, R.A. 2022. Vaccines and Liability. Hoover Institute (Accessed in August 2024.) https://www. hoover. org/research/vaccines-and-liability-0.

Fardet, A. & E. Rock 2014. Toward a New Philosophy of Preventive Nutrition: From a Reductionist to a Holistic Paradigm to Improve Nutritional Recommendations. *Advances in Nutrition* 5,4: 430 - 446. https://doi. org/10. 3945/an. 114. 006122.
<Go to ISI>://WOS:000339643300006. PMid:25022992 PMCid:PMC4085191

Feltham, E., L. Forastiere, M. Alexander & N.A. Christakis 2023. Mass Gatherings for Political Expression had no Discernible Association with the Local Course of the COVID-19 Pandemic in the USA in 2020 and 2021. *Nature Human Behaviour* 7,10: 1708-+. https://doi. org/10. 1038/s41562-023-01654-1.
<Go to ISI>://WOS:001040224100001. https://doi. org/10. 1038/s41562-023-01654-1 PMid:37524931

Fisher, D.A., T.R. Miller, J.W. Grube, C.L. Ringwalt, T. Achoki, T.P. Ngwato, L. Shilakoe & P. Mkhondo 2022. Locked Down: Economic and Health Effects of COVID-19 Response on Residents of a South African Township. *Global Social Welfare* 13. https://doi. org/10. 1007/s40609-022-00230-1. <Go to ISI>://WOS:000835567800001. PMid:35967248 PMCid:PMC9361952

Garcia, M.A., A.D. Thierry & C.B. Pendergrast 2022. The Devastating Economic Impact of COVID-19 on Older Black and Latinx Adults: Implications for Health and Well-Being. *Journals of Gerontology Series B-Psychological Sciences and Social Sciences* 77,8: 1501 - 1507. https://doi. org/10. 1093/geronb/gbab218. <Go to ISI>://WOS:000790119700001. PMid:34850887 PMCid:PMC8690256

Greene, J. 2021. Wait What? FDA Wants 55 Years to Process FOIA Request over Vaccine Data. Reuters (Accessed in August 2024.) https://www. reuters. com/legal/government/wait-what-fda-wants-55-years-process-foia-request-over-vaccine-data-2021-11-18/.

Greene, J. 2022. 'Paramount Importance': Judge Orders FDA to Hasten Release of Pfizer Vaccine Docs. Reuters (Accessed in August 2024.) https://www. reuters. com/legal/government/paramount-importance-judge-orders-fda-hasten-release-pfizer-vaccine-docs-2022-01-07/.

Guyatt, G. 1992. Evidence-based Medicine – A New Approach to Teaching the Practice of Medicine. *Jama - Journal of the American Medical Association* 268,17: 2420 - 2425. https://doi. org/10. 1001/jama. 1992. 03490170092032.
<Go to ISI>://WOS:A1992JV69400030. PMid:1404801

Hao, X.J., S.S. Cheng, D.G. Wu, T.C. Wu, X.H. Lin & C.L. Wang 2020. Reconstruction of the Full Transmission Dynamics of COVID-19 in Wuhan. *Nature* 584,7821: 420-+. https://doi. org/10. 1038/s41586-020-2554-8. <Go to ISI>://WOS:000559369500001. PMid:32674112

Herby, J., L. Jonung & S.H. Hanke 2022. *A Literature Review and Meta-Analysis of the Effects of Lockdowns on COVID-19 Mortality*. Johns Hopkins Institute for Applied Economics.

Herby. J., L. Jonung, S.H. Hanke 2023. *Did Lockdowns Work? The Verdict on COVID Restrictions — Institute of Economic Affairs*. IEA Publications.

Hobday, R.A. & J.W. Cason 2009. The Open-Air Treatment of PANDEMIC INFLUENZA. *American Journal of Public Health* 99: S236 - S242. https://doi. org/10. 2105/ajph. 2008. 134627. <Go to ISI>://WOS:000271218800006. PMid:19461112 PMCid:PMC4504358

Hoeg, T.B., S. González-Dambrauskas & V. Prasad 2023. Does Equipoise Exist for Masking Children for COVID-19? *Public Health in Practice* 6: 3. https://doi. org/10. 1016/j. puhip. 2023. 100428. <Go to ISI>://WOS:001133615500001. PMid:37744300 PMCid:PMC10511791

Hu, Y., L.C. Kong, T. Yao, X.D. Chen & W. Du 2021. Does Lock-down of Wuhan Effectively Restrict Early Geographic Spread of Novel Corona-virus Epidemic during chunyun in China? A Spatial Model Study. *Bmc Public Health* 21,1: 8. https://doi. org/10. 1186/s12889-021-10837-2. <Go to ISI>://WOS:000654914900007. PMid:33926395 PMCid:PMC8082222

Hurrell, M. 2020. Max Hurrell - ZOL, Unofficial Music Video by The Kiffness - YouTube.

Institute, S. 2023. Holistic Management ⋆ Savory Institute. Savory Institute. https://savory. global/holistic-management/.

Jakovljevic, M., S. Bjedov, N. Jaksic & I. Jakovljevic 2020. COVID-19 Pandemia and Public and Global Mental Health from the Perspective of Global Health Security. *Psychiatria Danubina* 32,1: 6 - 14. https://doi. org/10. 24869/psyd. 2020. 6. https://www. ncbi. nlm. nih. gov/pubmed/32303023. PMid:32303023

Jefferson, T., C. Del Mar, L. Dooley, E. Ferroni, L.A. Al-Ansary, G.A. Bawazeer, M.L. van Driel, S. Nair, R. Foxlee & A. Rivetti 2010. Physical Interventions to Interrupt or Reduce the Spread of Respiratory Viruses. *Cochrane Database of Systematic Reviews* 1: 85. https://doi. org/10. 1002/14651858. CD006207. pub3.

<Go to ISI>://WOS:000274654000038.

Jewett, C. 2020. FDA's Drug Industry Fees Fuel Concerns Over Influence – *The New York Times.* (Accessed in August 2024.) https://www. nytimes. com/2022/09/15/health/fda-drug-industry-fees. html.

Joubert, M., L. Guenther, J. Metcalfe, M. Riedlinger, A. Chakraborty, T. Gascoigne, B. Schiele, A. Baram-Tsabari, D. Malkov, E. Fattorini, G. Revuelta, G. Barata, J. Riise, J. T. Schroeder, M. Horst, M. Kaseje, M. Kirsten, M.W. Bauer, M. Bucchi, O. Wolfson, T.J. Chen & N. Flores 2023. 'Pandem-icons' - Exploring the Characteristics of Highly Visible Scientists during the COVID-19 Pandemic. *Jcom - Journal of Science Communication* 22,1: 24. https://doi. org/10. 22323/2. 22010204. <Go to ISI>://WOS:000922283100001.

Juul, F.E., H.C. Jodal, I. Barua, E. Refsum, O. Olsvik, L.M. Helsingen, M. Loberg, M. Bretthauer, M. Kalager & L. Emilsson 2022. Mortality in Norway and Sweden during the COVID-19 Pandemic. *Scandinavian Journal of Public Health* 50,1: 38 - 45. https://doi. org/10. 1177/14034948211047137. <Go to ISI>://WOS:000713730100001. PMid:34609261 PMCid:PMC8807990

Kamath, A., A. Yadav, J. Baghel & S. Mundle 2022. Locked Down: Experiences of Domestic Violence in Central India. *Global Health-Science and Practice* 10,4: 9. https://doi. org/10. 9745/ghsp-d-21-00630. <Go to ISI>://WOS:000865966400009. PMid:36041829 PMCid:PMC9426993

Kapitsinis, N. 2021. The Underlying Factors of Excess Mortality in 2020: A Cross-country Analysis of Pre-pandemic Healthcare Conditions and Strategies to Cope with COVID-19. *Bmc Health Services Research* 21,1: 19. https://doi. org/10. 1186/s12913-021-07169-7. <Go to ISI>://WOS:000714575800001. PMid:34736434 PMCid:PMC8568489

Kenny, C. 2023. 'Utterly appalling': Government Censored COVID Posts that were 'actually true' | *Sky News Australia*. https://www. skynews. com. au/opinion/chris-kenny/utterly-appalling-government-censored-covid-posts-that-were-actually-true/video/340e76e27e9f43a9830d2abc0c71be87.

Khanna, R.C., M.V. Cicinelli, S.S. Gilbert, S.G. Honavar & G.V.S. Murthy 2020. COVID-19 Pandemic: Lessons Learned and Future Directions. *Indian Journal of Ophthalmology* 68,5: 703 - 710.

https://doi. org/10. 4103/ijo. IJO_843_20. <Go to ISI>://WOS:000639424400007. PMid:32317432 PMCid:PMC7350475

Kisielinski, K., S. Wagner, O. Hirsch, B. Klosterhalfen & A. Prescher 2023. Possible Toxicity of Chronic Carbon Dioxide Exposure Associated with Face Mask Use, Particularly in Pregnant Women, Children and Adolescents – A Scoping Review. *Heliyon* 9,4: 18. https://doi. org/10. 1016/j. heliyon. 2023. e14117. <Go to ISI>://WOS:000998122500001. PMid:37057051 PMCid:PMC9981272

Lei, Q., Y. Li, H.Y. Hou, F. Wang, Z.Q. Ouyang, Y.D. Zhang, D.Y. Lai, J. L.B. Ndzouboukou, Z.W. Xu, B. Zhang, H. Chen, J.B. Xue, X.S. Lin, Y.X. Zheng, Z.J. Yao, X.N. Wang, C.Z. Yu, H.W. Jiang, H.N. Zhang, H. Qi, S.J. Guo, S.H. Huang, Z.Y. Sun, S.C. Tao & X. L. Fan 2021. Antibody Dynamics to SARS-CoV-2 in Asymptomatic COVID-19 Infections. *Allergy* 76,2: 551 - 561. https://doi. org/10. 1111/all. 14622. <Go to ISI>://WOS:000582534400001. PMid:33040337 PMCid:PMC7675426

Lin, X.S. & J. Guan 2022. 'Negative Efficacy' should have Stopped COVID Vaccine Recommendations in their Tracks | *The Epoch Times*. Epoch Health. https://www. theepochtimes. com/health/allowing-negative-efficacy-vaccines-upends-pre-pandemic-vaccine-standards-4889548.

Lintern, S. 2020. Coronavirus Vaccine: Pfizer given Protection from Legal Action by UK Government. Independent. co. uk (Accessed in August 2024.) https://www. independent. co. uk/news/health/coronavirus-pfizer-vaccine-legal-indemnity-safety-ministers-b1765124. html.

López-Castro, T., L. Brandt, N.J. Anthonipillai, A. Espinosa & R. Melara 2021. Experiences, Impacts and Mental Health Functioning during a COVID-19 Outbreak and Lockdown: Data from a Diverse New York City Sample of College Students. *Plos One* 16,4: 17. https://doi. org/10. 1371/journal. pone. 0249768. <Go to ISI>://WOS:000638119900003. PMid:33826654 PMCid:PMC8026074

Mahagamage, Y. & K. Marasinghe 2023. The Socio-economic Effects of COVID-19. *Saude E Sociedade* 32,1: 12. https://doi. org/10. 1590/S0104-12902022200961en. <Go to ISI>://WOS:000936803200001.

Mannan, K.A. & K.M. Farhana 2020. Knowledge, Attitude and Acceptance of a COVID-19 Vaccine: A Global Cross-Sectional Study. *International Research Journal of Business and Social Science* 6,4: 1 - 23. https://doi. org/10. 2139/SSRN. 3763373. https://papers. ssrn. com/abstract=3763373.

Markel, H., H.B. Lipman, J.A. Navarro, A. Sloan, J.R. Michalsen, A.M. Stern & M.S. Cetron 2007. Nonpharmaceutical Interventions Implemented by US Cities during the 1918 - 1919 Influenza Pandemic. *Jama - Journal of the American Medical Association* 298,6: 644 - 654. https://doi. org/10. 1001/jama. 298. 6. 644.
<Go to ISI>://WOS:000248574800025. PMid:17684187

Markov, P.V., M. Ghafari, M. Beer, K. Lythgoe, P. Simmonds, N.I. Stilianakis & A. Katzourakis 2023. The Evolution of SARS-CoV-2. *Nature Reviews Microbiology* 21,6: 361 - 379. https://doi. org/10. 1038/s41579-023-00878-2.
<Go to ISI>://WOS:000963720400001. PMid:37020110

Martin, D.E. 2022. Dr. David E. Martin PhD - Covid Summit - European Union Parliament May 2023. Rumble. com. https://rumble. com/v2ncp8w-dr-david-e. -martin-phd-covid-summit-european-union-parliament-may-2023. html.

Mazzocchi, F. 2012. Complexity and the Reductionism - Holism Debate in Systems Biology. *Wiley Interdisciplinary Reviews - Systems Biology and Medicine* 4,5: 413 - 427. https://doi. org/10. 1002/wsbm. 1181. <Go to ISI>://WOS:000307731200001. PMid:22761024

McChrystal, S., T. Collins, D. Silverman & C. Fussell 2015. *Team of Teams: New Rules of Engagement for a Complex World*. McChrystal Group.

Meng, C.L., S. Bannerman & E. Abrokwah 2022. Reviewing the Global Economic Impacts and Mitigating Measures of COVID-19. *Total Quality Management & Business Excellence* 33,13-14: 1573 - 1587. https://doi.org/10.1080/14783363.2021.1981130
<Go to ISI>://WOS:000704570700001.

Minnai, F., G. de Bellis, T.A. Dragani & F. Colombo 2022. COVID-19 Mortality in Italy Varies by Patient Age, Sex and Pandemic Wave. *Scientific Reports* 12,1: 9. https://doi. org/10. 1038/s41598-022-08573-7.
<Go to ISI>://WOS:000770396200039. PMid:35301379
PMCid:PMC8929285

Morawska, L. & D.K. Milton 2020. It Is Time to Address Airborne Tranmission of Coronavirus Disease 2019,COVID-19). *Clinical Infectious Diseases* 71,9: 2311-2313. https://doi. org/10. 1093/cid/ciaa939.
<Go to ISI>://WOS:000605984800024. PMid:32628269
PMCid:PMC7454469

Morsy, H., L. Balma & A.N. Mukasa 2021. 'Not a good time': Assessing the Economic Impact of COVID-19 in Africa Using a Macro - Micro

Simulation Approach. *African Development Review - Revue Africaine De Developpement* 33: S17-S30. https://doi. org/10. 1111/1467-8268. 12526. <Go to ISI>://WOS:000651402200001. PMid:34149238 PMCid:PMC8207119

Norberg, J. 2023. Sweden during the Pandemic | Cato Institute. Cato Institute. https://www. cato. org/policy-analysis/sweden-during-pandemic#.

Ogrodniczuk, J.S., M. Sivagurunathan, D. Kealy, S.M. Rice, Z E. Seidler & J.L. Oliffe 2023. Suicidal Ideation among Men during COVID-19: Examining the Roles of Loneliness, Thwarted Belongingness & Personality Impairment. *Scandinavian Journal of Psychology* 64,4: 401 - 408. https://doi. org/10. 1111/sjop. 12904. <Go to ISI>://WOS:000928746500001. PMid:36744862

Onyema, E.M., N.C. Eucheria, F.A. Obafemi, S. Sen, F.G. Atonye, A. Sharma, A.O. Alsayed 2020. Impact of Coronavirus Pandemic on Education. *Journal of Education and Practice* 11: 108 - 121. https://doi. org/10. 7176/JEP/11-13-12. https://www. iiste. org/Journals/index. php/JEP/article/view/52821.

Ozili, P.K. & T. Arun 2020. Spillover of COVID-19: Impact on the Global Economy. *SSRN*: 1-23. https://doi. org/10. 2139/SSRN. 3562570. https://papers. ssrn. com/abstract=3562570. https://doi. org/10. 2139/ssrn. 3562570

Panda. 2023. PANDA: Independent Insights to Empower Societies. PanData. https://pandata. org/.

Pirkis, J., D. Gunnell, S. Shin, M. Del Pozo-Banos, V. Arya & P.A. Aguilar 2022. Suicide Numbers during the First 9 - 15 Months of the COVID-19 Pandemic Compared with Pre-existing Trends: An Interrupted Time Series Analysis in 33 Countries. *eClinicalMedicine* 51: 101573. https://doi. org/10. 1016/j. eclinm. 2022. 101573. http://www. thelancet. com/article/S2589537022003030/fulltext http://www. thelancet. com/article/S2589537022003030/abstract https://www. thelancet. com/journals/eclinm/article/PIIS2589-5370(22)00303-0/abstract.

Pirkis, J., A. John, S. Shin, M. DelPozo-Banos, V. Arya, P. Analuisa-Aguilar, L. Appleby, E. Arensman, J. Bantjes, A. Baran, J.M. Bertolote, G. Borges, P. Brecic, E. Caine, G. Castelpietra, S.S. Chang, D. Colchester, D. Crompton, M. Curkovic, E.A. Deisenhammer, C. Du, J. Dwyer, A. Erlangsen, J.S. Faust, S. Fortune, A. Garrett, D. George, R. Gerstner, R. Gilissen, M. Gould, K. Hawton, J. Kanter, N. Kapur, M. Khan, O.J.

Kirtley, D. Knipe, K. Kolves, S. Leske, K. Marahatta, E. Mittendorfer-Rutz, N. Neznanov, T. Niederkrotenthaler, E. Nielsen, M. Nordentoft, H. Oberlerchner, R.C. O'Connor, M. Pearson, M.R. Phillips, S. Platt, P.L. Plener, G. Psota, P. Qin, D. Radeloff, C. Rados, A. Reif, C. Reif-Leonhard, V. Rozanov, C. Schlang, B. Schneider, N. Semenova, M. Sinyor, E. Townsend, M. Ueda, L. Vijayakumar, R.T. Webb, M. Weerasinghe, G. Zalsman, D. Gunnell & M.J. Spittal 2021. Suicide Trends in the Early Months of the COVID-19 Pandemic: An Interrupted Time-series Analysis of Preliminary Data from 21 Countries. *Lancet Psychiatry* 8,7: 579 - 588. https://doi. org/10. 1016/s2215-0366(21)00091-2. <Go to ISI>://WOS:000750668400001. PMid:33862016

Ponte, B., J. Costas, J. Puche, D. de la Fuente & R. Pino 2016. Holism versus Reductionism in sSupply Chain Management: An eEconomic Analysis. *Decision Support Systems* 86: 83 - 94. https://doi. org/10. 1016/j. dss. 2016. 03. 010. <Go to ISI>://WOS:000376808400008.

Prasad, R.R. 2020. Media Freedom and COVID-19. international. gc. ca (Accessed in August 2024.) https://www. international. gc. ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/policy-orientation-COVID-19. aspx?lang=eng.

Radonovich, L.J. Jr., M.S. Simberkoff, M.T. Bessesen, A.C. Brown, D.A.T. Cummings, C.A. Gaydos, J.G. Los, A.E. Krosche, C.L. Gibert, G.J. Gorse, A.C. Nyquist, N.G. Reich, M.C. Rodriguez-Barradas, C.S. Price, T.M. Perl & Pect investigators Res. 2019. N95 Respirators vs Medical Masks for Preventing Influenza Among Health Care Personnel: A Randomized Clinical Trial. *JAMA* 322,9: 824 - 833. https://doi. org/10. 1001/jama. 2019. 11645. https://www. ncbi. nlm. nih. gov/pubmed/31479137. PMid:31479137 PMCid:PMC6724169

Rainer, K., V. Fischer, A. Leidwein & G. Neubauer. 2022. Ethics and Human Aspects in Pandemic Management. *Ercim News*,131: 28-29. <Go to ISI>://WOS:000870514500016.

Reuters 2020. Minibus Drivers in South Africa Strike Over Coronavirus Funding. Reuters (Accessed in August 2024.) https://www. voanews. com/a/COVID-19-pandemic_minibus-drivers-south-africa-strike-over-coronavirus-funding/6191527. html.

Ribatti, T. 2021. Reductionism, Vitalism & Holism. *Critical Reviews in Eukaryotic Gene Expression* 31,3: 1-3.

Richardson, S., J.S. Hirsch, M. Narasimhan, J.M. Crawford, T. McGinn, K.W. Davidson, Covid-Research Consortium the Northwell, D.P. Barnaby, L.B.

Becker, J.D. Chelico, S.L. Cohen, J. Cookingham, K. Coppa, M.A. Diefenbach, A.J. Dominello, J. Duer-Hefele, L. Falzon, J. Gitlin, N. Hajizadeh, T.G. Harvin, D.A. Hirschwerk, E.J. Kim, Z.M. Kozel, L.M. Marrast, J.N. Mogavero, G.A. Osorio, M. Qiu & T.P. Zanos 2020. Presenting Characteristics, Comorbidities & Outcomes among 5700 Patients Hospitalized With COVID-19 in the New York City Area. *JAMA* 323,20: 2052-2059. https://doi. org/10. 1001/jama. 2020. 6775. https://www. ncbi. nlm. nih. gov/pubmed/32320003. https://doi. org/10. 1001/jama. 2020. 6775
PMid:32320003 PMCid:PMC7177629

Rimšēvičs, I. 2021. COVID-19 Mitigation Measures, Economic Impact and Factors in Recovery. *Regional Formation & Development Studies* 34: 179 - 190. https://doi. org/10. 15181/RFDS. V34I2. 2254.

Rodriguez, N.J.I. 2017. A Comparative Analysis of Holistic Marine Management Regimes and Ecosystem Approach in Marine Spatial Planning in Developed Countries. *Ocean & Coastal Management* 137: 185-197. https://doi. org/10. 1016/j. ocecoaman. 2016. 12. 023. <Go to ISI>://WOS:000394077000017.

Russell, C.D., N.I. Lone & J.K. Baillie 2023. Comorbidities, Multimorbidity and COVID-19. *Nature Medicine* 29,2: 334 - 343. https://doi. org/10. 1038/s41591-022-02156-9. <Go to ISI>://WOS:001188221300002. PMid:36797482

Savory, A. & T. Butterfield 2016. *Holistic Management: A Commonsense Revolution to Restore Our Environment*. Savory Institute.

Savory, A. & J. Butterfield 1999. *Holistic Management: A New Framework for Decision Making*. Island Press.

Secrets, Open 2023a. Moderna Inc Lobbying Profile • OpenSecrets. Accessed Open Secrets. https://www. opensecrets. org/federal-lobbying/clients/summary?id=D000073555.

Secrets, Open 2023b. Pfizer Inc Profile: Summary • OpenSecrets. Open Secrets. https://www. opensecrets. org/orgs/pfizer-inc/summary?id=D000000138.

Seminara, G. & M. Bolla Pittaluga 2012. Reductionist versus Holistic Approaches to the Study of River Meandering: An Ideal Dialogue. *Geomorphology* 163: 110 - 117. https://doi. org/10. 1016/j. geomorph. 2011. 06. 037. <Go to ISI>://WOS:000306449400010.

Showalter, M. 2023. As COVID Recrudesces, Major Meta-study Questioning Lockdowns is Censored. (Accessed in August 2024.) https://www. americanthinker.

com/blog/2023/09/as_covid_recrudesces_major_metastudy_questioning_lockdowns_is_censored. html.

Sigalos, M. 2020. Covid Vaccine: You can't Sue Pfizer or Moderna over Side Effects. CNBC (Accessed in August 2024.) https://www. cnbc. com/2020/12/16/covid-vaccine-side-effects-compensation-lawsuit. html.

Smiley, L. 2020. 27 Days in Tokyo Bay: What Happened on the Diamond Princess. Wired. com.

Spaull, N. & S. van der Berg 2020. Counting the Cost: COVID-19 School Closures in South Africa and its Impact on Children. *South African Journal of Childhood Education* 10,1: 13. https://doi. org/10. 4102/sajce. v10i1. 924. <Go to ISI>://WOS:000599158400001.

Spear, R. 1986. Reagan Signs Bill on Drug Expors and Payment for Vaccine njuries. *New York Times.* (Accessed in August 2024.) https://www. nytimes. com/1986/11/15/us/reagan-signs-bill-on-drug-exports-and-payment-for-vaccine-injuries. html.

Staff, University Herald 2024. Johns Hopkins to Pay Students Back $6M in Tuition for Semester of Pandemic Remote Learning. universityherald. com (Accessed in August 2024.) https://www. universityherald. com/articles/79155/20240801/johns-hopkins-university-pandemic-tuition-refunds-maryland-lawsuit. htm.

Team, The 2023. Secretive COVID Disinformation Unit Worked with Security Services. *The Telegraph.* (Accessed in August 2024.) https://www. telegraph. co. uk/news/2023/09/01/secretive-covid-disinformation-unit-security-services/.

Tellis, G. J., A. Sood, S. Nair & N. Sood 2023. Lockdown Without Loss? A Natural Experiment of Net Payoffs from COVID-19 Lockdowns. *Journal of Public Policy & Marketing* 42: 133 - 151. https://doi. org/10. 1177/07439156221143954. https://journals. sagepub. com/doi/10. 1177/07439156221143954. PMid:38603285 PMCid:PMC9836842

Todaro, J.M. 2020. A Study Out of Thin Air | MedicineUncensored. Medicine Unsensored. https://archive. is/OHo20.

UF. 2024. ACQUIRE - Find the Evidence - Evidence-Based Dentistry - Guides. UF at University of Florida. https://guides. uflib. ufl. edu/c. php?g=627277&p=4384372.

UPMC 2022. COVID-19 Vaccination. What is an Emergency Use Authorization, EUA)?. upmc. com (Accessed in August 2024.) https://share. upmc. com/2020/12/what-is-emergency-use-authorization/.

Van Damme, W., R. Dahake, A. Delamou, B. Ingelbeen, E. Wouters, G. Vanham, R. Van De Pas 2020. The COVID-19 Pandemic: Diverse Contexts: Different Epidemics - How and Why? *BMJ Global Health* 5: e003098. https://doi. org/10. 1136/BMJGH-2020-003098. https://gh. bmj. com/content/5/7/e003098 https://gh. bmj. com/content/5/7/e003098. abstract. PMid:32718950 PMCid:PMC7392634

Verschuur, J., E.E. Koks & J.W. Hall 2021. Global Economic Impacts of COVID-19 Lockdown Measures Stand out in High-frequency Shipping Data. *PLoS One* 16,4: e0248818. https://doi. org/10. 1371/journal. pone. 0248818. https://www. ncbi. nlm. nih. gov/pubmed/33852593. PMid:33852593 PMCid:PMC8046185

Wang, S.S.Y. & W.Z.Y. Teo 2021. Equitable and Holistic Public Health Measures During the Singaporean COVID-19 Pandemic. *Ann Glob Health* 87,1: 45. https://doi. org/10. 5334/aogh. 3244 https://www. ncbi. nlm. nih. gov/pubmed/34046308 PMid:34046308 PMCid:PMC8139311

Wasserman, D., M. Iosue, A. Wuestefeld & V. Carli 2020. Adaptation of Evidence-based Suicide Prevention Strategies During and After the COVID-19 Pandemic. *World Psychiatry* 19,3: 294-306. https://doi. org/10. 1002/wps. 20801. https://www. ncbi. nlm. nih. gov/pubmed/32931107. PMid:32931107 PMCid:PMC7491639

WHO 2020. Voluntary Contributions by Fund and by Contributor, 2020. WHO. (Accessed in August 2024.) https://iris. who. int/handle/10665/359079.

WHO 2023. COVID-19 Cases | WHO COVID-19 Dashboard. WHO (Accessed in August 2024.) https://data. who. int/dashboards/covid19/cases?n=c.

WHO 2023a. Programme Budget 2022 – 2023, approval, WHA74.3. WHO. https://www. who. int/publications/i/item/programme-budget-2020-2021-approval-(wha74. 5).

Wicky, P. H., C. Dupuis, C. Cerf, S. Siami, Y. Cohen, V. Laurent, B. Mourvillier, J. Reignier, D. Goldgran-Toledano, C. Schwebel, S. Ruckly, E. de Montmollin, N. Buetti & J.F. Timsit 2023. Ventilator-associated Pneumonia in COVID-19 Patients Admitted in Intensive Care Units: Relapse, Therapeutic Failure and Attributable Mortality – A Multicentric

Observational Study from the OutcomeRea Network. *Journal of Clinical Medicine* 12,4. https://doi. org/10. 3390/jcm12041298. https://www. ncbi. nlm. nih. gov/pubmed/36835834.
PMid:36835834 PMCid:PMC9961155

Wood, N. 2020. Who Pays Compensation if a COVID-19 Vaccine has Rare Side-effects? Sydney University, Opinion.
https://www. sydney. edu. au/news-opinion/news/2020/10/20/who-pays-compensation-if-a-covid19-vaccine-has-rare-side-effects. html.

Wu, R. 2022. An Empirical Investigation of the Economic Impacts of COVID-19: Micro-level Evidence from Europe. Routledge.
https://doi. org/10. 2139/ssrn. 4164266

Yang, X., Y. Yu, J. Xu, H. Shu, J. Xia, H. Liu, Y. Wu, L. Zhang, Z. Yu, M. Fang, T. Yu, Y. Wang, S. Pan, X. Zou, S. Yuan & Y. Shang 2020. Clinical Course and Outcomes of Critically Ill Patients with SARS-CoV-2 Pneumonia in Wuhan, China: A Single-centered, Retrospective, Observational Study. *Lancet Respiratory Medicine* 8,5: 475 - 481.
https://doi. org/10. 1016/S2213-2600(20)30079-5.
https://www.ncbi.nlm.nih.gov/pubmed/32105632 PMid:32105632

Younos, T., J. Lee & T. Parece. 2018. Twenty-first Century Urban Water Management: The Imperative for Holistic and Cross-disciplinary Approach. *Journal of Environmental Studies and Sciences* 9,1: 90 - 95.
https://doi. org/10. 1007/s13412-018-0524-3.

Zhou, M., X. Zhang & J. Qu. 2020. Coronavirus Disease 2019, COVID-19: A Clinical Update. *Front of Medicine* 14,2: 126 - 135.
https://doi. org/10. 1007/s11684-020-0767-8.
https://www. ncbi. nlm. nih. gov/pubmed/32240462.
PMid:32240462 PMCid:PMC7115348

Zinecker, M., K. Doubravský, A. P. Balcerzak, M. P. Pietrzak & M. Dohnal. 2021. The COVID-19 Disease and Policy Response to Mitigate the Economic Impact in the Eu. *Technological and Economic Development of Economy* 27,3: 742-762.
https://doi. org/10. 3846/tede. 2021. 14585

Professor Gert (H.G.) Kruger
Catalysis and Peptide Research Unit
University of KwaZulu-Natal
Durban, South Africa
Kruger@ukzn. ac. za

Colleen Aldous
University of KwaZulu-Natal
Clinical Medicine and Health Sciences
Durban
South Africa
Aldousc@ukzn. ac. za

## Acknowledgement of Reviewers

We wish to acknowledge the participation of the following reviewers in the production of this volume of the *Alter*nation African Scholarship Book Series.

Prof. Igor Balyuk – Financial University under Government of the Russia Federation, balyuk@bk.ru or iabalyuk@fa.ru

Dr. David Gochenemi, Postdoctoral fellow, University of South Africa

Prof Nirmala Gopal, University of KwaZulu-Natal, Gopal@ukzn.ac.za

Ms. Melissa Hathaway – Harvard Kennedy School, https://www.hks.harvard.edu/about/melissa-hathaway

Dr. Sokfa John, https://www.conflictdynamics.co.za/Mediators/Mediator/11161

Dr. Vicent Mbonye – Management College of Southern Africa (MANCOSA), vicent.mbonye@mancosa.co.za

Dr. Timothy Obaje – Varsity College, tobaje@varsitycollege.co.za

Dr. Ojochenemi J. David – Durban University of Technology

Prof. Joelien Pretorius – University of Western Cape, jpretorius@uwc.ac.za

Prof. Johannes, A. Jannie Smit – University of KwaZulu-Natal, smitj@ukzn.ac.za

**BRICS**
**Peace, Security, and Economy**
**Research Intersections**

*Alter*nation African Scholarship Book Series #21 (2025)

## Advance Recommendations

The *BRICS: Peace, Security, and Economy Research Intersections* brings together critical and diverse scholarship that reviews the past and informs the future manifestation of the BRICS community, specifically its underestimated role in international peace and security. The volume is a welcome addition to the growing literature on alternative iterations of global governance.

**Professor Joelien Pretorius**
Position: Departmental Chair, University of the Western Cape.
Research Interests: Nuclear disarmament and non-proliferation, Africa and the nuclear order, Security Studies https://www.uwc.ac.za/study/all-areas-of-study/departments/department-of-political-studies/people

The *BRICS Peace, Security, and Economy Research Intersections* effectively presents a meticulously organised and analytically nuanced exploration of digital sovereignty within the BRICS nations. The editors demonstrate a discerning selection of contributions that illuminate each state's unique strategic orientation while simultaneously unpacking the wider ramifications for global peace and security dynamics. The collection offers a sophisticated and multifaceted perspective on how emerging powers are reshaping the digital governance landscape. It stands as an invaluable and timely resource for scholars critically examining the evolving architecture of international security.

**Professor Dr. I.A. Balyuk,** is Dr. of Sciences (Economics), at the Financial University under the Government of the Russian Federation, Department of World Economy and World Finance, Leningradsky Avenue, Moscow, Russian Federation. https://en.fa.ru/university/; and https://en.fa.ru/university/history/

UNIVERSITY OF KWAZULU-NATAL | INYUVESI YAKWAZULU-NATALI | COLLEGE OF HUMANITIES
NATIONAL INSTITUTE FOR THE HUMANITIES AND SOCIAL SCIENCES
SABTT South African BRICS Think Tank