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].

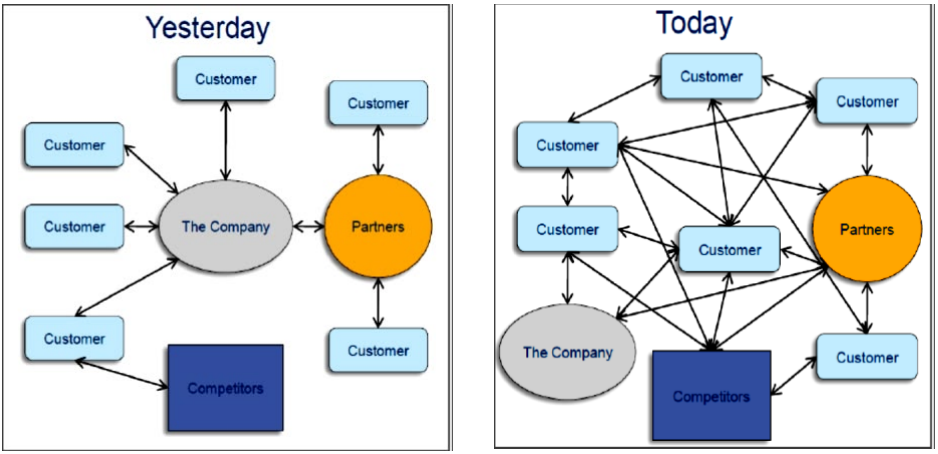

Figure 1. A shift from Company-centric to consumer-centric logic
Source: Dervojeda, Kristina *et al.* (2014)

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

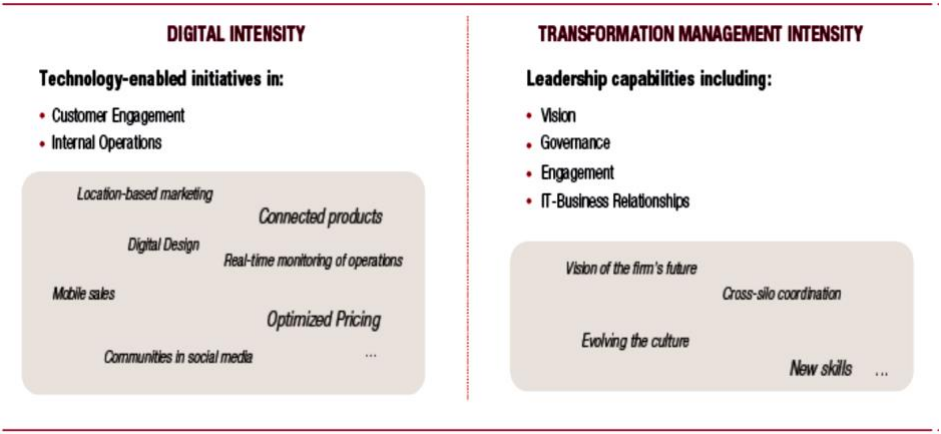

Figure 2. The What-and-How of Digital Transformation – Two Dimensions of Digital Intensity

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].

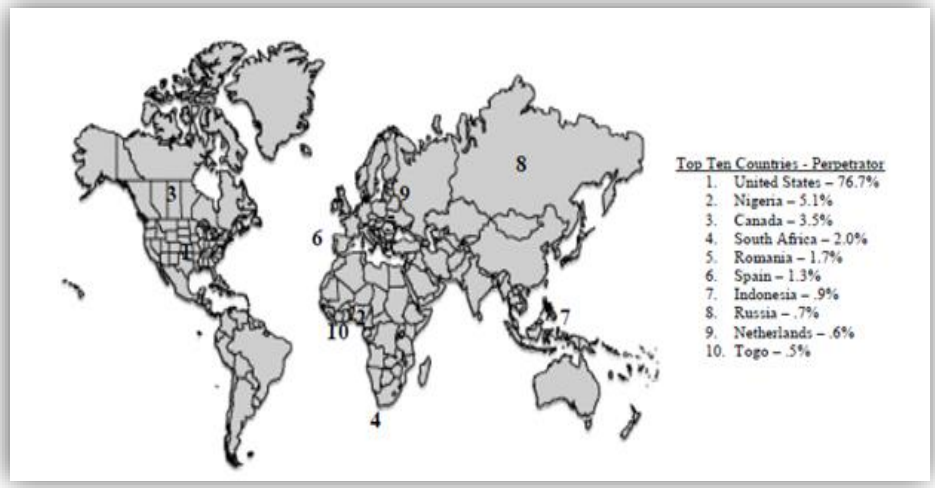

Figure 3. Top 10 states and country perpetrators - IC3 reports

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 • Public Exposure of the Private Information • Espionage • Interference with Police Operations and Sabotage • Defacing to Cause Embarrassment or Retaliation • Retribution • Profit • Notoriety • Disinformation	• Hacktivists • State Actors • Criminal Organizations • Terrorist Organizations • Purposeful or Accidental Insider • Individuals	• Personnel • Organizational Barriers • Information Networks & Systems • Public-Facing Websites • Data Storage Devices • Social Media Accounts • Communications Centers, Systems, Equipment and Applications • Wireless Devices • 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.

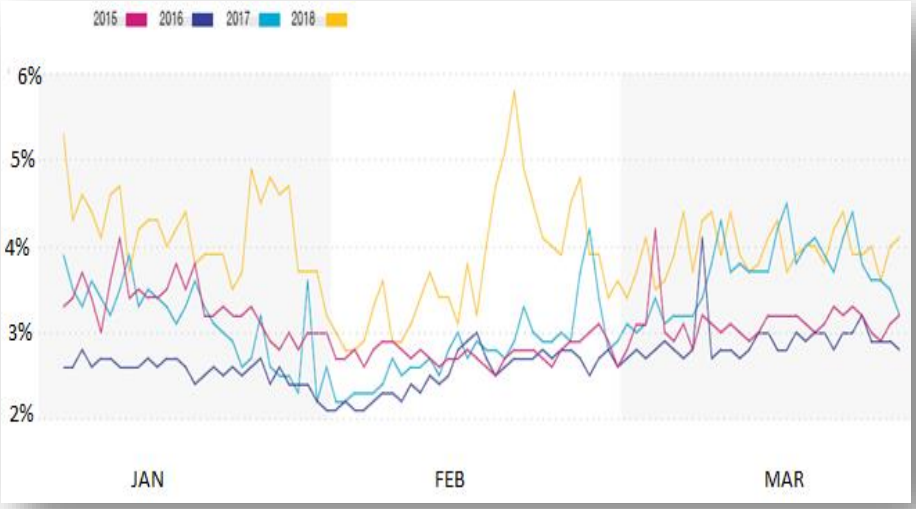

Figure 4. Q1 Daily Attack Rate 2015 to 2018
Source: 2018 CYBERCRIME REPORT - (ThreatMetrix Digital Identity Network 2018)[4]

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.

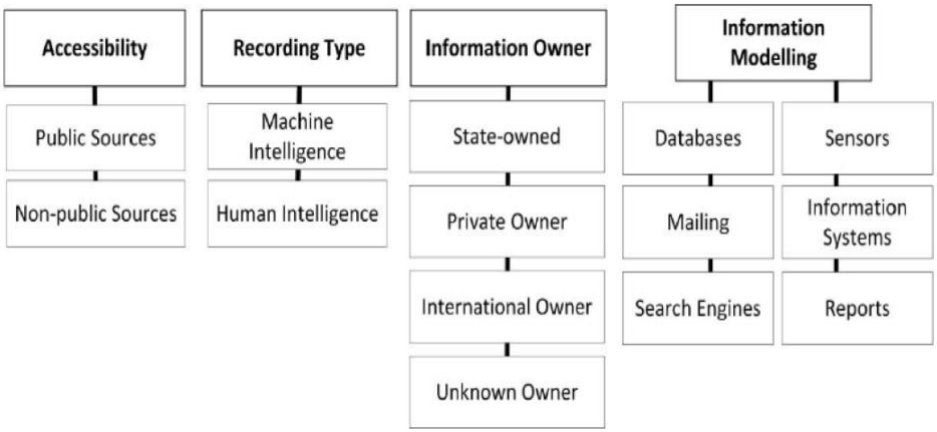

Figure 5. Categorization of information sources. Source: Pahi *et al*. (2017)

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 4.97×10^5 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.

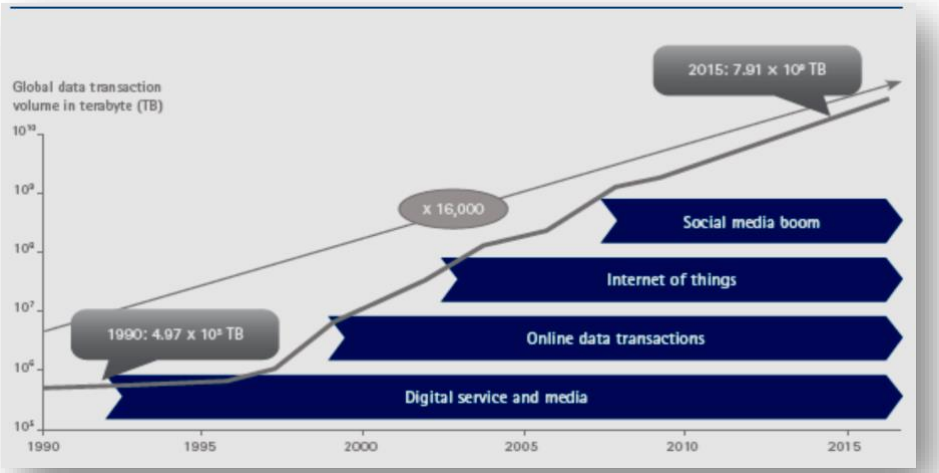

Figure 6. Source: comScore; Facebook; Sandvine: 'Information White Paper' 2011; Sandvine: 'Digital Contents White Paper' 2010; METI E-Commerce survey; IDC; consumer research; BCG analysis

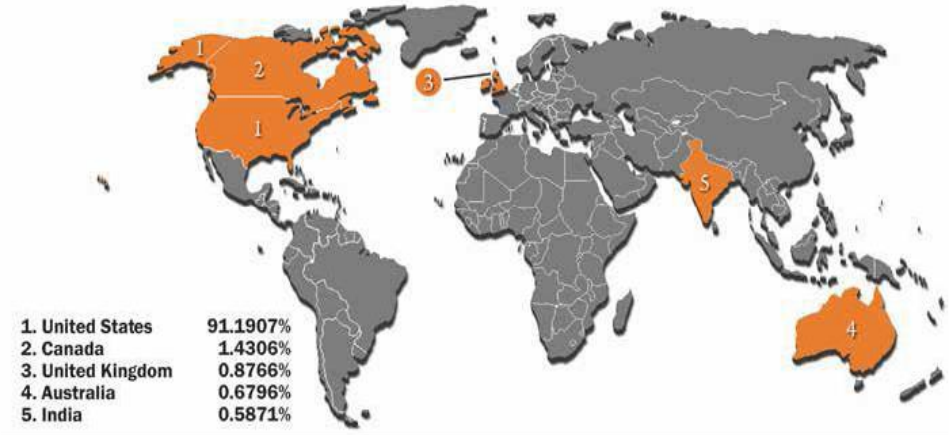

Figure 7. Top 5 Countries by Count: Victim Complainants (Numbered by Rank) 2012. Source FBI quoted in Verma and Sharma 201

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?

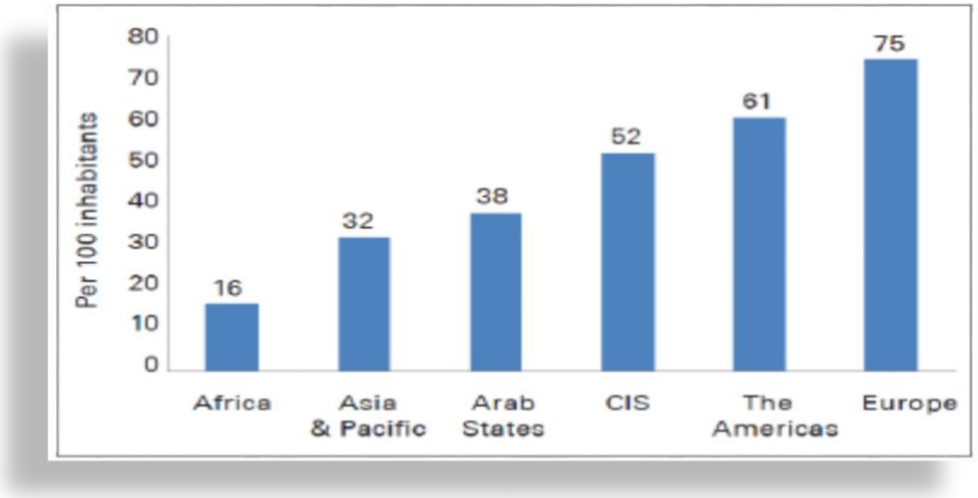

Figure 8. Diffusion of internet across the world. Source: Dervojeda *et al.* 2014.

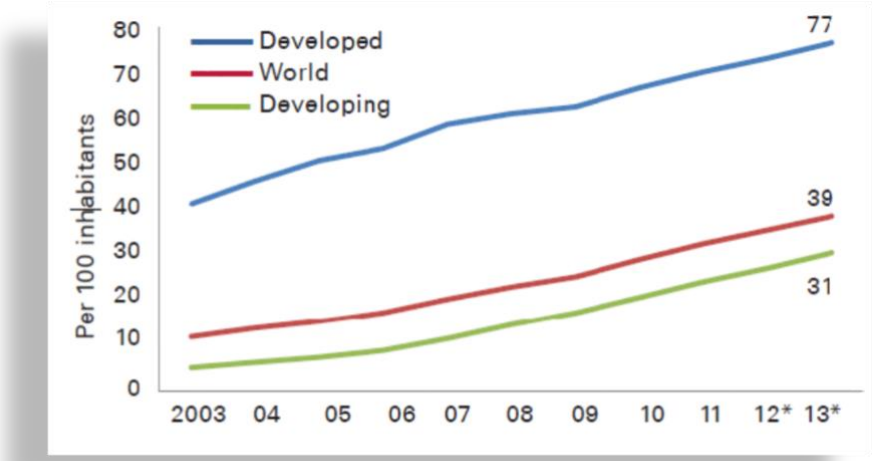

Figure 9. Diffusion of internet across the world.
ITU World Telecommunication/ICT indicators database captured from Dervojeda *et al.* (2014). Note: * Estimate

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'.

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.

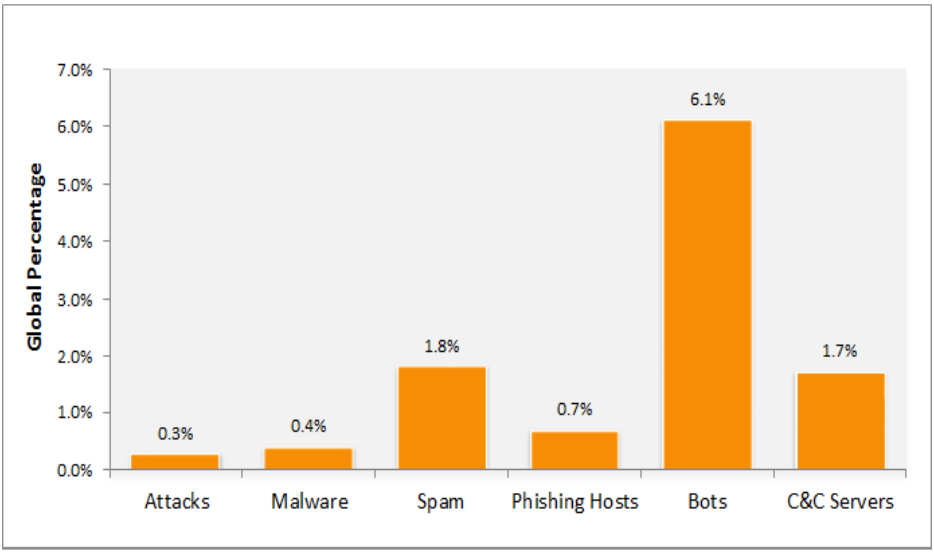

Figure 11. Malicious Activity Originating from Africa

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