JoMUN XVI

Forum: Disarmament Commission

Issue: Improve African governmental safeguards against cybersecurity threats

Student Officer: Shareef R. Jabba

Position: Deputy Secretary-General

"Following two decades of near stagnation, Africa's growth performance has improved hugely since the start of the 21st century" – The 2013 Economic Report on Africa. Since the early 2000's, the continent of Africa as a whole has continuously experienced sustained growth, accompanied by a rapid increase of commodities. Furthermore, organizations such as the African Development Bank and publications including The International Business Times and The Economist have emphasized that a number of the world's most rapidly growing economies are situated in Africa.

The aphorism, 'Africa rising' is prominently reflected through Africa's growing middle class and the continuous implementation and embracement of mobile technology throughout the continent. Based on data collected by the International Telecommunications Union (ITU), in 2013, the number of individuals with a mobile subscription reached 63%. Furthermore, according to the ITU, in 2013 the number of people using the internet in Africa comprise of around 16 percent of the continent's population.

Challenges arise as a result of the continued rapid development in the technological sectors within African countries. There are a variety of risks and vulnerabilities that arise from increasing technological exposure but one risk that requires immediate attention is that of cybercrime.

Cybercrime
Cybercrime, also known as computer-oriented crime, is a crime that is associated with a network and computers. The computer may be used to conduct the crime or may be the target itself.

Malicious Software (Malware)
Malware, short for malicious software, is used to describe a variety of intrusive software's including scareware, adware, ransomware, spyware, worms, trojan horses, and a number of other hostile and harmful viruses/programs.

Cybersecurity
Cybersecurity, also known as computer security and IT security is the defense against the damage and theft to a computer's software, information, and hardware. Furthermore, cybersecurity involves preventing the misdirection or disruption of a provided technological service.

Cyber espionage
Cyberespionage, also known as cyberspying, is the act of obtaining confidential information without the knowledge of that information's holder. This act can be performed by individuals, groups, and even governments. Cyber espionage is carried out for either personal, political,

groups, and even governments. Cyber espionage is carried out for either personal, political, economic, or military gain. Cyber espionage is practiced in networks and computers through proxy servers, malicious software, and a variety of cracking techniques which include but are not limited to, spyware and trojan horses.

Network
A network in the context of this issue is a number of interconnected operations, machines, and computers.

Infringement
"The act of breaking the terms of law" – Wikipedia

Data
General information including statistics or facts collected for analysis or reference.

According to a report published in 2013 by Symantec, although cybercrime is a growing phenomenon, "cybersecurity experts estimate that 80 percent of personal computers on the African continent are infected with viruses and other malicious software" (United Nations Economic Commission for Africa). As stated previously, multiple countries in Africa are in a state of rapid development. This position makes these various countries prone to threats posed by cybercriminals as African networks have extremely weak information and network security. For example, South Africa has a substantial number of cybercrime victims and lose around R2.2 billion a year as a result of cyber-attacks. Furthermore, according to the Norton Cyber-Crime Report, South Africa has the third highest number of cyber victims in the world.

Large and small businesses in Africa are also being targeted. According to the Symantec report previously mentioned, the number of African cyberattacks in 2012 increased by 42 percent. Of this 42 percent, 31 percent of them are characterized as cyberespionage. Although South Africa has the highest number of cybercrime victims, Nigeria is currently the largest source of spiteful Internet activities. A number of major African cities including Lagos, Nairobi, Johannesburg, and Cairo have experienced a doubling in the rate of cyber-connected disturbances.

Cybercrime continues to develop into further complexities thus requiring further enforcement and development of cybersecurity. This can be seen through information and communications technologies (ICTs). The 2013 Westgate Mall shooting in Nairobi as well as multiple Boko Haram and Al-Qaida attacks highlight the usage of information and communications technologies. These attacks are detrimental to the development of African nations and setback economic growth. To expand on this, not only did 67 people die in the Westgate shooting incident, but Kenya also lost approximately $200 million in tourism revenue.

"The Norton Cybercrime Report 2012 indicated that direct financial losses totaled an average $197 per victim worldwide, while globally a grand $110 billion in direct financial loss was recorded" (United Nations Economic Commission for Africa). Furthermore, studies conducted by the International Data Group Connect show that there is a strong relationship between the strength of a nations cybersecurity and its economic growth. Another study by the International Data Group Connect shows that on average, the Nigerian economy loses $200 million to cybercrimes annually; the South African economy loses $573 million, and the Kenya economy loses approximately $36 million.

Considering that cybercrimes transcend literal borders, it is very difficult to prevent crimes

Considering that cybercrimes transcend literal borders, it is very difficult to prevent crimes such as the loss of personal data, and intellectual property infringement. African governments lack the financial and technical capacity to oversee electronic exchanges that may be a threat to national security. Put simply, the primary challenges facing African countries are:

- Poor security provisions, unable to adequately control and efficiently prevent cybersecurity risk.
- A prominent inability to advance legal frameworks regarding cybersecurity. A survey conducted by the ECA showed that although a number of African countries attempted to propose legislation regarding cybersecurity, the level of deployment of these suggested security systems was considerably low.
- Very few cybersecurity initiatives across Africa have properly been implemented. This issue is transnational and thus should be dealt with in a more comprehensive manner.

Egypt
Egypt has a 'computer emergency response team' (EG-CERT) that aids and supports multiple entities in the ICT division within its country. In the Global Cybersecurity Index of 2017, Egypt is ranked 14th globally.

Rwanda
Rwanda is recognized for ranking highly in regard to the organization of its cybersecurity that concerns itself with both the private and public sector of the country. Rwanda is ranked 36th globally but 3rd in Africa.

Kenya
Kenya is known for its effectivity in finding efficient ways to cooperate and this can be seen through the National Kenya Computer Incident Response Team Coordination Centre. Kenya is ranked 45th globally in the 2017 Global Cyber Security Index.

Uganda
"This East African country has a Global Cyber Security Capacity Centre that has facilitated a self-assessment of cybersecurity capacity of the Republic of Uganda." (IT News Africa) Uganda is currently ranked at 50th globally and 7th in Africa.

Morocco
As a member of the ITU-IMPACT initiative, Morocco has access to a variety of cybersecurity services. Unlike many African countries, Morocco has an official cybersecurity framework which is aimed at practicing and implementing internationally recognized cybersecurity ideals. Morocco is ranked 49th globally.

South Africa
Being a prominent victim of Cybercrime, South Africa created the national cybersecurity hub which allows for collaboration between civil society, government, and industry regarding anything cybercrime related. "The cybersecurity hub is mandated by the National Cybersecurity Policy Framework (NCPF) that was passed by Cabinet in 2012" (IT News Africa). South Africa is ranked 58th globally and 8th in Africa.

The NATO Cooperative Cyber Defence Centre of Excellence - CCDCOE
This organization is an interdisciplinary and multinational hub centered around cyber defense knowledge. The Centre organizes the annual conference CyCon as well as "the world's largest and most complex international technical cyber defense exercise, Locked Shields" (CCDCOE). The international involvement allows the CCDCOE to have an international perspective when observing cyber defense.

Symantec

Symantec is an organization that assists individuals and organizations to manage and protect confidential information. Symantec is recognized as the global leader in security innovation. Symantec also publishes the annual Internet Security Threat Report.

2013 The estimated cost of cybercrime reaches 3.8 million Euros in the Ivory Coast.

2013 Zambian commercial banks are defrauded of over $4 million. This was an act of cybercrime which involved foreign nationals as well as local Zambians.

2014 According to Kaspersky, 49 million cyber attacks occur in the first three months of 2014 in Africa. The majority of these cyber attacks are taking place in Kenya, South Africa, Algeria, and Egypt.

2014 McAfee calculates that South African companies have lost over $500 million as a result of cybercrimes.

2014 A hacker going by the name of Yunus Incredibl hacked a total of six Senegalese government sites.

2015 The rapid spread of a form of cybercrime known as ransomware. Kaspersky detected this form of malware in over 200 countries and territories.

2015 “Kenya Cyber Security Report 2015 points out that in 2012, cybercriminals were opportunists by nature, or computer enthusiasts seeking to impress, but that they’ve now become hardened professionals, whose attacks have very specific aims” (Sci Dev Net)

2015 In Kenya, a survey showed less than 5 percent of organizations had adequately prepared themselves with the tools necessary in order to properly protect their databases from the threats of cybercrime.

2015 Anonymous Senegal attacks the Ministry of Livestock and Animal Production as well as major sites of the State Information Technology Agency (ADIE)

2015 Hackers attempt four times to steal $24 million from the coffers of the Ugandan central bank. These hackers targeted the accounts of the agencies who held big shares of the state budget. Information also reveals that these hackers had accomplices in the civil service.

The Africahackon Conference –
This conference addresses topics that are associated with the offensive and defensive aspects of cybersecurity. This event attracts talented professionals who are willing to share knowledge and interact with the individuals and organizations that come to learn. The event is also aimed at promoting career paths centered around cybersecurity.
https://africahackon.com/

CyberCon Africa-
This conference is aimed at "bringing like-minded people to deal with the issues of cyber vulnerability and protection of all sectors from cybercrimes" (CyberCon). The conference has many attendees who are experts in the cyber field. This cyber event is centered around providing insight on building resiliency towards cybercrime and learning how to prevent such malicious occurrences.
http://www.cyberconafrica.org/
International Information Security South Africa Conference -
This conference aims at uniting the efforts of academia and the industry in order to come up with effective cybersecurity solutions that will benefit society as a whole.
http://www.infosecsa.co.za/

UN Draft Resolution on Guidelines to Cybersecurity and Data Protection -
This resolution is one of the many that concerns itself with the issue of cybersecurity. In this case, the resolution has a specific scope which is intelligent transport systems, also known as automated driving. For further research on specific resolutions, use the UN Document Database (linked in the appendix of this research report).
https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/440/66/pdf/G1644066.pdf?OpenElement

---

Attempts by the FBI –

The Federal Bureau of Investigation (FBI) is a domestic intelligence and security service for the United States. They acknowledge the serious nature of cybercrimes and are continuously looking for ways to catch cybercriminals worldwide. Although the FBI operates within the United States, they also concern themselves with international matters especially cybercrime as it is a transnational issue.

https://archives.fbi.gov/archives/news/testimony/the-fbis-efforts-to-combat-cyber-crime-on-social-networking-sites

United Nations involvement: Global Programme on Cybercrime –

Loide Lungameni, Chief of the Organized Crime and Illicit Trafficking Sector in the UN Office on Drugs and Crime (UNODC) stated that "cybercrime has become an established threat to the security of States and individuals alike". The United Nations acknowledges the true nature of cybercrime as a rising threat to communities and organizations and is committed to combatting such threats.

https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

European Union efforts -
The European Union has taken initiative in combatting cybercrime through a variety of ways. For example, the European Union recognizes the importance of legislative action. Additionally, with the fact that cybercrime is an international issue, the European Union cherishes and promotes the importance of cross-sectoral international cooperation.

Furthermore, the European Union is investing time and effort into capacity building which is the process of developing and strengthening skills.
https://www.thegfce.com/news/news/2017/05/31/the-eus-efforts-in-fighting-cybercrime

---

National network infrastructures –
Infrastructures that promote cross cooperation between the civil society, government, the research community, and the industry would strongly support the battle against cybercrimes. This method promotes open knowledge engagement through combining and sharing information regarding technological development.

Emergency readiness –
In order to promote national synergy on cybersecurity, a national computer emergency readiness and response team would strongly benefit the affected community. This would not only promote cybersecurity but would also establish trust between civil society and the government in regards to the safety of their confidential data and information. This readiness team should not only aid in emergency situations but should also strive to promote the sharing of information as well as the collection of intelligence on countermeasures against cybercrime.

Call center –
A call center which promotes direct interaction between the victims and the assistants would aid in the fight against cybercrime. This call center would allow the victims of cybercrime to report their issue as well as receive assistance. The staff at the call center should be professionally trained and adequately equipped with the materials and resources necessary to aid anyone in a threatening situation. Establishing a website and a toll-free number with these call centers would be convenient.
Investment in research –
"Knowledge and information serve as a direct way of empowering countries and their citizens" (United Nations Economic Commission for Africa). As can be seen from the multiple cyber attacks in Africa, it is clear that there is a general lack of knowledge and information regarding cybersecurity in the continent. Investment in resources in materials in order to better the community's knowledge of cybersecurity is an imperative necessity. Investment should also be channeled in to research as there are many bright minds in Africa who could positively contribute to the development and advancement of cybersecurity.

Education –
The use of technology is growing at an exponential rate in Africa. With the youth and younger generations being raised in such a time, it is important that they are mentally and physically equipped with the required knowledge and tools to efficiently and effectively protect their information. Further initiatives should be created that target the promotion of internet safety, child protection, and general social security. Furthermore, "facilitation of secure ICT access for users is of paramount importance" (United Nations Economic Commission for Africa).

"Cybercrime in Africa: Facts and Figures." *SciDev.Net Sub-Saharan Africa*, Sci Dev Net , www.scidev.net/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html.

"DOHA: UN Conference Weighs Efforts to Combat Cybercrime, Create Safer Digital World | UN News." *United Nations*, United Nations, news.un.org/en/story/2015/04/496242-doha-un-conference-weighs-efforts-combat-cybercrime-create-safer-digital-world.

"The EU's Efforts in Fighting Cybercrime: Putting Together Legislative Action, Cross-Sectoral and International Cooperation, as Well as Capacity Building." *News Item | Global Forum on Cyber Expertise*, Ministry of Foreign Affairs, 21 Aug. 2017, www.thegfce.com/news/news/2017/05/31/the-eus-efforts-in-fighting-cybercrime.

"The FBI's Efforts to Combat Cyber Crime on Social Networking Sites." *FBI*, FBI, 28 July 2010, archives.fbi.gov/archives/news/testimony/the-fbis-efforts-to-combat-cyber-crime-on-social-networking-sites.

crime-on-social-networking-sites.
"Global Cybersecurity Index (GCI) 2017." *Global Cybersecurity Index (GCI) 2017*, www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.
"Tackling The Challenges of Cyber Security In Africa." *Tackling The Challenges of Cyber Security In Africa*, 2014, www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf.
"Top 10 African Countries Committed to Cybersecurity ." *Top 10 African Countries Committed to Cybersecurity* , IT News Africa , www.itnewsafrica.com/2017/07/top-10-african-countries-committed-to-cybersecurity/.

Official UN Document System

- Can be used to find multiple resolutions relating to the topic of concern
- https://documents.un.org/prod/ods.nsf/home.xsp

Global Cyber Security Index (GCI) 2017

- https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

The Tallinn Manual Process

- Comprehensive analysis of international laws application on cyberspace
- https://ccdcoe.org/tallinn-manual.html

UN Policy Brief on the challenges of cybersecurity

- Very helpful, thorough, and simple information regarding the challenges and potential solutions around cybersecurity in Africa
- https://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf