New threats to peace and Security: Extent to which new security threats of Cyber security have affected economic and human security in East Africa

By Moses Kulaba, *Governance and economic analysis centre, Dar es Salaam-Tanzania*

Cyber security or attacks by using highly sophisticated technology and cyber space to penetrate, modify, adulterate or alter existing ICT infrastructure to inflict significant, damage to a country, an installation, equipment, companies or individuals. According to NATO cyber insecurity is crippling of vital defence and military installations and capabilities to protect human security[1]

Effects of Cyber Security on Human and Economic Security

From a military or defense security perspective, cyber security threat from the following angles or forms

- **Cyberterrorism** is the disruptive use of information technology by terrorist groups to further their ideological or political agenda. This takes the form of attacks on networks, computer systems and telecommunication infrastructures.
- **Cyberwarfare** involves nation-states using information technology to penetrate another nation's networks to cause damage or disruption. In the U.S. and many other nations, cyberwarfare has been acknowledged as the fifth domain of warfare (following land, sea, air and space).
- Cyberwarfare attacks are primarily executed by hackers who are well-trained in exploiting the intricacies of computer networks, and operate under the auspices and support of nation-states. Rather than "shutting down" a target's key networks, a cyberwarfare attack may intrude into networks to compromise valuable data, degrade communications, impair such infrastructural services as transportation and medical services, or interrupt commerce.
- **Cyberespionage** which is the practice of using information technology to obtain secret information without permission from its owners or holders. Cyberespionage is most often used to gain strategic, economic, political or military advantage, and is conducted using cracking techniques and malware[2].

[1] https://www.nato.int/cps/en/natohq/opinions_147867.htm
[2] https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security

In recent past cyber-attacks have become quite rampant. In 2008 the Estonian attack in which the entire Estonian Government agencies, financial institutions and broadcasters were jammed by Russian cyber attacker was a good example. In 2010 the reports of attacks on googles mails by Chinese hackers and Sony pictures were a clear reminder of the extent of the risk posed by Cyber security.

Cyber-attacks have capabilities to disrupt government systems, transport and communication infrastructure and defence capabilities.

However, from a human and economic security perspective, cyber insecurity has largely affected social and economic sectors. Cyber security has globalised or regionlaised organized crime[3]. According to the UK government's Cyber Security Breaches Survey 2017 found that the average cost of a cyber security breach for a large business was £19,600 and for a small to medium-sized business was £1,570[4]. According to a CISCO Annual report on cyber security, over one third of organizations that experienced breach in 2016 reported loss of substantial customer opportunity and revenue loss in more than 20% [5]

Effects of cybercrime of human and economic security in East Africa

Experts have described the East African digital economy as weak and vulnerable to multiple cyber attacks

> ***"Essentially, in terms of cyber resilience, the Kenyan digital economy can be likened to a slow, plump gazelle stumbling through the 'cyber savanah'' in the full view of an agile, informed and hungry cyber predator, keen to sink their teeth into their sumptuous prize"***

In 2016, African countries reportedly lost USD2bln in cyber-attacks. Remittance based economies, which depend on electronic wire transfers of money from its foreign sources and nationals living abroad via the international financial system were the worst hit[6]

Effects on Financial systems

Financial transactions such as banking and money transfer services have been the largest targets affecting millions of people. In East Africa it was reported that Kenya was the worst

[3] http://www.biztechafrica.com/article/cybercrime-now-top-five-economic-threat-east-afric/9951/
[4] https://www.itgovernance.co.uk/what-is-cybersecurity
[5] https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf
[6] David Bunei; Connected Summit 2017

affected with a total estimated of loss of USD 171Mln while Tanzania lost USD85million and Uganda lost USD 35million in its financial sector.[7]

Tanzania's cyber security report for 2016 warned of critical dangers facing the country. According to the report technology adoption is driving business innovation and growth in Tanzania, while at the same time, exposing the Country to new and emerging cyber security threats. Terrorists, spies, hackers, fraudsters are increasingly motivated to target Tanzania's Information, Communication and Technology (ICT) infrastructure due to the value of information held within it, the report indicated.

One of the major risks was lack of awareness amongst technology users. According to the report over 1.6 million Internet Portals (IPs) were publicly accessible and over 138,000 network security events were reported.

Effects of exposure through interconnected and domestic gadgets

Cybercrime has reduced human security risk through exposure to interconnected things such as medical devices, smart TVs, cars and other gadgets. Research has found potential vulnerabilities in dozens of devices such as insulin pumps, and implantable defibrators. Hundreds of connected TVs are potentially vulnerable to click fraud, botnets, data, ransomware. Cybercriminals have developed mechanisms to remotely take control of personal gadgets such as remotely opened cars, personal computers.

Threat to privacy and confidentiality

There is a security risk of breach of confidentiality and personal privacy on vital confidential documents and personal data. As governments become digitalized through the drive for e-government, confidential government documents and personal details of its citizens are now more exposed to cybercrime. From passports, birth certificates, medical reports, pension numbers and personal IDs are now interlinked via the electronic networks

Costly policing and administration in cyber defence

Fighting cybercrime is very costly to police and enforcing cyber security diverts the already constrained government resources away from financing vital social services such as education and health. According to cybersecurity readiness report very few governments and companies can afford to invest in highly sophisticated cyber security defence systems. The Kenyan Cyber Security report highlighted that about 44% of financial institutions run on a paltry cyber security budget of USD1-1000 annually. About 33% of financial institutions in Kenya have spent

[7] https://www.standardmedia.co.ke/business/article/2001235820/kenya-worst-hit-in-east-africa-by-cyber-crime

nothing on all matters of cyber security[8].There are limited skills to manage and address it and keep ahead of cyber criminals, the report warns.

Regional attempts to counter and fight cybersecurity

Regional initiatives to combat cybercrime have been initiated through specialized units now established in the military and police forces of the East African states. However, they are still ill trained and under equipped to effectively contain the threats.

In conclusion, it is evident that the threats of piracy and cyber security has been increasing and pause a major threat to human and economic security of the region. Piracy and Cybercrime are highly organized global crimes with vast networks operating miles away. The weak counter measures and lack of adequate resources to counter these threats suggest that these will remain security threats to the region for longtime.

Indeed, given the increasing threat that cyber-crime has generated it is probable to suggest that future wars may/will not be fought on the battle fronts but in cyber space. Soldiers of the future will not be Generals commanding battalions and platoons of mobiles soldiers marching across battle fields. The generals of the future will be technologically savy individuals sitting in high-tech offices and issuing commands to remote computers, gadgets and robots deployed to engage targets thousands of miles away.

References:

https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security

http://www.biztechafrica.com/article/cybercrime-now-top-five-economic-threat-east-afric/9951/

https://www.itgovernance.co.uk/what-is-cybersecurity

https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf

https://www.standardmedia.co.ke/business/article/2001235820/kenya-worst-hit-in-east-africa-by-cyber-crime

[8] ibid