Image of dangerous cyber threats.

On June 19 this year, the Ministry of Information ,Communications and Technology in collaboration with the ICT Authority Kenya exclusively released a comprehensive cybersecurity document titled, 'National Cybersecurity Strategy 2014'.

In it, the Ministry Principal Secretary Mr. Joseph Tiampati Ole Musuni re-affirms State commitment to fighting Cyber insecurity. He notes that, "As Kenya matures into an information society, the nation faces an increasingly evolving Cyber threat landscape."

Indeed, statistics provided by the same ministry portray a rather grim picture. Just for instance, in 1980-85, the two most dominant Cyber threats were password guessing and self replicating code. However, over the years, the most common cybsecurity concerns have been and still are password cracking, exploiting known vulnerabilities, disabling audits, and back doors. In the 1990s, hijacking sessions, "sweepers", "sniffers", "stealth diagnosis", "packet spoofing" as well as "intruder toolkits" were and still are diseases of our time.

Come 1995-2000, automated probes/scans,denial of service, and distributed attacks were and still are disturbing the Cyberspace. In 200-2005, commercialization of hacking, blended attacks, mutable malware, "phishing" and infrastructure attacks rocked the cyberworld.

The year 2006 heralded much more advanced attacks and threats which, despite concerted efforts, have never been successfully combated and tamed. In addition, Kenya's 2014 cyberspace users are still grappling with "Botnets", converged attacks, cyber-based terrorism, organized crime, nation-state cyber-warfare, "next generation" denial of service as well as targeted malicious code.

Our Government has determined these cyber attacks to come from "hacktivists" seeking to publicize political views, from criminal organizations seeking financial gain, from terrorist groups seeking to inflict economic or political damage, or from state-sponsored intelligence and security organizations advancing their own economic or national security aims.

Moreover, many of the attacks involve extremely sophisticated technological and social engineering techniques.The rest, despite their execution with low-technology penetrations (such as insider threats), they are not far from being dangerous.

To make the picture clearer, here is a case study of the most exacting and impacting cyberattacks : in May 31 2005, an article in *the Guardian* reports 21 executives and private detectives arrested on suspicion of using Trojan virus to infiltrate their rivals' computer systems.

In November 2013, Capital FM's website ran a sad story of several Kenyans conned money by hackers who hacked into their friends' Facebook accounts.

January 18 2013 was another Kenyan case of "Mobile Spoofing" : according to an article in *Humanipo*, mobile money agents, particularly those of M-Pesa, were losing an estimated US$13,00 a month to "spoofs", after several fraudsters posed as mobile network operator's engineers defraud them.The particulars of the attack were that the fraudsters, who pretended to be upgrading the system, impersonated Safaricom employees to trick the M-Pesa agents into giving them details about their businesses.They then transferred the money in the agent's accounts into their accounts and withdrew it from other outlets.

Sadly, it was the same year Kenya's Chief Justice's email accounts were hacked into,according to *the Standard.* Also see *Humanipo*. And the list goes on and on.

Nevertheless, despite the discouraging state of affairs,the Government has taken crucial steps to markedly improve the nation's cybersecurity posture. The Kenya Information and Communications Act 2014, the formation of the National Kenya Computer Incident Response Team Coordination Center (KE-CIRT/CC), and the establishment of the National Certification Authority Framework-which provides a foundation for public key infrastructure implementation, are some of the revolutionary initiatives.

Other pertinent moves entail partnership with regional and international cybersecurity bodies and forums including the International Telecommunications Union (ITU) and the East Africa Communications Organization (EACO).

Even-so, the Government admits that while these activities and initiatives will help it evolve its cybersecurity posture, overall, the nation's cybersecurity situation will still be relatively immature in the face of the growing complexity and sophistication of cyber threats. Hence the need for a National Cybersecurity Strategy, which is expected to mature the cybersecurity landscape by providing a strategic cybersecurity direction.

According to Information, Communications and Technology ministry PS Joseph Tiampati Ole Musuni, the strategy was developed "in direct support of the national priorities and ICT goals defined in Vision 2030".

This Strategy indeed defines Kenya's cybersecurity vision, key objectives, as well as ongoing Government commitment to support national priorities by encouraging ICT growth and aggressively protecting critical information infrastructures.

But a robust cybersecurity policy, legal and regulatory framework that provides direction, roles, responsibilities, goals, resources, and governance plans in the creation of a strong cybersecurity doctrine is essential to translating strategic cybersecurity intent into a viable operating model.

Thus the GoK Regulatory, Policy, and Legal Framework provide essential inputs to the National Cybersecurity Strategy via the following measures: analyzing GoK's baseline cybersecurity governance model; evaluating GoK's cybersecurity maturity; highlighting national cybersecurity master plan considerations and providing recommendations for a GoK Regulatory, Policy and Legal Framework.

The Legal Framework will in turn identify needed laws,regulations and policy; define governance roles and responsibilities; prescribe measures to secure critical cyber infrastructure; the framework will also involve the private sector in policy development; facilitate international cooperation; define and protect against cybercrime; will balance information security and privacy considerations, and promote secure online transactions through trusted identities.

Having looked at the policies that augment the National Cybersecurity Strategy, it now becomes crucial that we take a close look at the blueprint. To promote Government's commitment to cybsersafety, the Strategy includes four important goals:

The top most is to '**enhance the nation's cybersecurity posture**'. Here, GoK is "taking steps to increase the security and resilience of its critical information infrastructure to protect its government, citizens and residents, and corporations from cyber threats and to reap the socio-economic benefits of cyberspace".

The cybersecurity document reveals that the Government will effectively achieve the foregoing aim through a "coordinated effort with other countries to increase the security of global cyberspace as a whole, when the Government secures critical infrastructures, applications, and services". And a host of other measures.

Number two in the Strategy is **building 'national capability**' through awareness and training. As a result, GoK is increasing cybersecurity consciousness by "informing and educating the public and workforce on how to secure the national cyberspace. This will be implemented most effectively through partnerships with other government organizations, the private sector, and academia in a bid to ensure that "people with cybersecurity responsibilities possess the appropriate level of cyber qualifications and

competencies". This all about human capital development,education and training, and strategic communication. As the Government is working with academia, we expect "cybersecurity curriculum for higher education", and "specialized training programs to ensure competency building for cybersecurity professionals". And so on.

In fostering '**information sharing and collaboration**', GoK intends to develop the required laws, regulations and policies for securing the nation's cyberspace; balance information security, privacy considerations and economic priorities. This is only possible if and when the Government solicits stakeholder input and feedback, as appropriate.

In fact, the Government echoes, "successful implementation of the Strategy requires the sharing of cybersecurity information in a trusted and structured manner". And it will develop and manage a secure information-sharing capability to promote knowledge and lessons learned among relevant stakeholders.

Lastly, the Strategy's fourth aim is to '**provide national leadership**' through a "single,unified agenda that will guide all relevant national stakeholders". Hence the ICT Ministry will continue to refresh the Strategy as required and establish a tactical roadmap for achieving national cybersecurity objectives. Using the Strategy in conjunction with the Cybersecurity Master Plan to identify and implement relevant cybersecurity initiatives, is also part of the deal.

Eventually, reveals the ICT PS,"cybersecurity is a shared responsibility. The Government will continue to partner with the private sector, academia, and other non-government entities to implement our strategy in the most efficient and effective way possible."

"We have every confidence that we will meet these challenges together and and increase recognition of Kenya as a trusted partner and cybersecurity leader in the East African Community, Africa, and the world," he adds.

About the Writer

Moses Omusolo is the Social Media Manager, C4DLab