Dr. Tony Omwansa at a past Cyber-security training event in July.

From November 5 to 7, 2014, C4DLab was conducting its second edition of the Cybsersecurity training at the University of Nairobi in conjunction with ICT Authority. The training, having been previously rescheduled from October 1 this year, had attracted participants from various parts of the country.

Preparing the ground for the three-day coaching was Dr. Tony Omwansa, the Computing for Development (C4D) Lab's Coordinator.

Dr. Omwansa took the eager trainees through various essential elements of the course such as "cyber-security terminology", "cyber-attack characteristics", about those who initiate them, about "economics of cyber-security", "cyber-security policy", "trends in cyber-security", "Kenya's Cyber-security strategy" as well as barriers to improving the same.

Other key facilitators included Dr. Chris Chepken who is a UoN Chiromo ICT lecturer as well as Mr. Evans Kahuthu, the ICT Authority's Project Manager.

By the end of the third day, Dr. Chepken had taken the 14 participants through " hacking", which he said begins with information gathering initiated mostly by the insiders of an organization. Hacking techniques, threats, detection, prevention, incident handling, business continuity planning and disaster recovery were also the province of Mr. Chepken.

The Project Manger for ICT Authority on the other hand trained on the aspects of "information security" , " web application security" and "network security" .

Meanwhile, the following themes emerged at the successful seminar: Dr. Tony Omwansa and colleagues taught that the cyber-security issue revolved around certain key aspects of computing which the trainees came to know as hardware, software as well as communications.

Further, everyone had to know, information security depended heavily on confidentiality, integrity and availability. That protection of the same ranged from the physical, personal, to the organizational.

A cyber-attack, the deliberate or accidental exploitation of computer systems and networks to compromise data and lead to cyber-crimes, was shown to have the following characteristics: one, it is

inexpensive. Meaning that many attack tools can be purchased for a modest price or downloaded for free from the Internet.

Furthermore, such an attack is ‘easy’- it takes an attacker with only basic skills to cause significant damage. On ‘effectiveness’, the participants came to learn that even a minor attack can cause extensive damage.

Lastly, given that an attacker can evade detection and prosecution especially by hiding their tracks through a complex web of computers as well as exploiting gaps in domestic and international legal regimes, the incident was to be labeled ‘low-risk’.

Cyber-attacks, the students came to learn, are perpetrated by ‘hacktivists’ seeking to publicize things such as political views. Criminal organizations on the other hand, might be seeking financial gain.

To inflict economic or political damage, terrorist groups were found to use the cyberspace unethically and illegally. Sate-sponsored intelligence and security organizations do attack the cyber world with an aim to advance their own economic or national security aims.

Hence the following trends in cyber-security from 1980-2014: in 1980-85, the two most dominant cyber-threats were password guessing and self replicating code.

From left is Dr. Chris Chepken, UoN ICT lecturer and Mr. Evans Kahuthu, ICT Authority's Project Manager.

However, over the years, the most common cyber-security concerns have been and still are password cracking, exploiting known vulnerabilities, disabling audits, and back doors. In the 90s, 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 cyber world. In 2000-2005, commercialization of hacking, blended attacks, mutable malware, “phishing” and infrastructure attacks rocked the virtual landscape.

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 cyber-space 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.

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 even clearer, here is a case study of the most exacting and impacting cyber-attacks : in May 31, 2005, an article in *the Guardian* reported 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”. The particulars of the attack were that the fraudsters, pretending 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 from the agents’ 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.

Alternatively, the grievous impact of cyber-crime was presented to the training attendees as shown below:

- cyber-crime- $400 billion in 2011 globally (according to World Bank)
- piracy- about $8 billion in 2005

- car crashes- $ 168 billion in 2010 (USA only)
- illegal drug trafficking- $600 billion in 2012 (according to the United Nations)
- the US loses about $100 billion annually and spends $400 billion a year on research and development.
- the US estimates that $100 billion in losses from cyber-espionage translate to 508, 000 lost jobs.

Eventually, the expert trainers would leave their students yearning for the implementation of a robust and fruitful cyber-security policy as well as strategy.

Fortunately, Kenya's Cyber-security Strategy was found by the inductees to be addressing four key concerns: the nation's cyber-security posture was to be enhanced by the protection of critical information infrastructure; national capability could be realized by creating awareness and initiating key collaborations; information sharing would be fostered through the solicitation of stakeholder input/feedback. Lastly, 'national leadership' was to be achieved when the National Cyber-security Strategy and plan were developed, implemented and refreshed.

But the vision would only be realized if key challenges such as misaligned incentives, information asymmetry, values and ethical issues, the disabling legal framework/standards, and so on were tackled.