CYBER TERRORISM

Cyber terrorism is the intentional use of computers and information technology to cause harm or further social, ideological, religious, political or similar objectives. This is effected by hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, Distributed Denial-of-service (DDoS) attacks, or terror threats made via electronic communication. Cyber terrorism is a critical threat to national security and public policy and is not confined to state-actors alone but also individuals and organizations. The risk level posed is determined by the capability of the threat and the vulnerabilities existent in our systems.

Three levels of cyber terror capability namely

- **Simple-Unstructured:** The capability to conduct basic hacks against individual systems using tools created by someone else. There is little target analysis, command and control or learning capability.
- **Advanced-Structured:** The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The aggressor possesses an elementary target analysis, command and control, and learning capability.
- **Complex-Coordinated:** The capability for a coordinated attack capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Usually at a state-sponsored level, there is ability to create sophisticated hacking tools, conduct target analysis, command and control, and overall organization learning capability.

Examples of cyber terrorism incidents are **Estonia 2007**, where the Baltic state of Estonia was target to a massive denial-of-service attack that ultimately rendered the country offline and shut out from services dependent on Internet connectivity for three weeks in the spring of 2007. The infrastructure of Estonia including everything from online banking and mobile phone networks to government services and access to health care information was disabled for a time. The tech-dependent state was in severe problem and there was a great deal of concern over the nature and intent of the attack. While **New York Times, Twitter and Huffington Post 2013, l**ost control of some of their websites after hackers supporting the Syrian government breached the Australian Internet company that manages many major site addresses. The Syrian Electronic

Army, a hacker group claimed credit for the hacks in a series of Twitter messages. Electronic records showed that NYTimes.com, the only site with an hours-long outage, redirected visitors to a server controlled by the Syrian group before it went dark.

The increasing dependence on ICT to control and manage critical infrastructure such as public utilities, electricity, water, telecommunications, finance and others renders these infrastructure to cyber terror. Threats issued to US and Britain on attacks on critical information infrastructure is an indication that terrorism is taking a new dimension, hence need for the Government of Kenya and the Ministry of Defense to secure the critical infrastructure against cyber terrorism.

Cyber terrorism can be prevented or minimized by:

- Securing systems with hardware and software protection, installation of intrusion detection systems and respond immediately to any intrusions
- Setting up public-private partnership to track threats will build capacity
- Creating a firm security policy: that includes training of employees to guard against such things as opening email attachments or responding to messages from unknown sources, use and management of strong passwords that include a combination of numbers, letters and other characters
- Conducting regular checks to make sure security precautions are followed, security threats updates and application of filters to screen out suspicious material or messages from known sources of threats such as specific countries
- Testing the defenses regularly to routinely try identify vulnerabilities either software or hardware and sealing these vulnerabilities.

The key attribute to preventing cyber terrorism is awareness because all a cyber terrorist looks for is access into a network and you could just be providing them with it through poor cyber hygiene.

Lois Bosire

Assistant Director/ICT

Ministry of Defence