CYBER WARFARE IN KENYA

PAST, CURRENT AND FUTURE TRENDS.

COLLINS ODUOR BUNDE

I132/0858/2013

0713175471

collinsbunde@gmail.com

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

JARAMOGI OGINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

Abstract

Cyberwarfare are actions by nations states to penetrate another nations networks or computers, it's with the objective of achieving information superiority by tampering with a perceived adversaries' information systems while offering protection for one's information based systems, networks and infrastructure. With the rapid growth of internet and ICT in Kenya that has delivered economic growth to unprecedented scales by facilitating seamless connectivity globally.(Serianu, 2016).This study seeks to, showcase how Kenya has advanced in cyberwarfare and to identify the targets of the cyberwarfare activities in Kenya and finally it identifies the existing impact of cyberwarfare in Kenya, with a consideration of the past, present and future trends.

1.0 Introduction

Cyberspace is a new domain of warfare that in recent years has joined the traditional arenas of land, sea, air, and space. The study that follows describes the unique characteristics of this new domain of warfare, offers fresh interpretations of familiar concepts, and surveys landmark events and organizations in the field of cyberspace in Israel and abroad. Modern nations and advanced militaries around the world are intensifying their activities in cyberspace, which simultaneously constitutes a source of power and a soft underbelly

Cyberwarfare are the actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption, it also includes non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations.

The much hyped progress in Africa is indelibly linked with information technology and notably technology has its negatives such as malware, and cybercrime threats. Unlike in the western world where the difficulty mainly lies in the constant upgrade of legacy systems, many Africa countries just provide a virtual blank slate, with lack of enough knowledge to extend their potential (IDG CONNECT, 2016)

With the spike in the IT sector, concerns about security are on the rise. The greater accessibility only earns more opportunities for cyber criminals to exploit the novice users and their lack of experience with technology this leads to increases in the chances of encountering malwares and viruses. Unprepared governments and businesses will also suffer in the hands of the hackers manipulate the lack of awareness and inadequate protection put in place. The aim of this paper is to investigate the how Kenya is coping with the rise of cyberwarfare the existing trends.

Discussion

Advancement in Cyberwarfare in Kenya.

Past

Aside from cyber-crime, average hacktivists have targeted Kenya for fun and practice. In 2012 an Indonesian student-hacker known as ‘Direxer’, took down 103 government of Kenya web sites overnight. The hacker had taken down these web sites following tutorials from the forum called the Indonesian Security Forum Code. The following year another hacker attacks, disabled the official police site, and two university hacks that changed exam results, while yet another attack cleared student fees. This clearly showed a cause of concern for the government.

Present

According to Federov, (2016) from his excerpt from the business daily. A group of around 77 Chinese were found to be perpetrating cyber espionage in Kenya the group appeared to be manufacturing ATM cards was suspected to be involved in internet fraud and money laundering and by extension cyber-espionage .

Kenya Cybercrime Bill

The Kenya and Computer Crimes Bill aims at sealing the legislative loopholes that make it possible for cyber fraudsters to perpetrate offences in the country. In June 2013, a committee was formed to spearhead efforts against cybercrime under the Communications Act of Kenya. The Kenya Information and Communications bill 2013 incorporated and defined the term cyber security in the amendments further stipulating the penalties of the crimes for both individuals as well as organizations found committing them. This is a good indicator that the Kenyan government has taken the necessary preliminary steps towards securing our information, communication and technology infrastructure.

Agreement with ITU

The Communications Authority of Kenya (CA) signed an agreement with International Telecommunications Union (ITU) on 30th July 2015 for technical assistance to fight cybercrime in Kenya. The agreement is meant to specifically provide enhanced technical support to the National Computer Incident Response Team - Coordination Centre (KE-CIRT/CC) which operates in connection with the network of Computer Incident Response Team Centers (CIRTs) ("CAK", 2016).

The targets for the cyberwarfare activities

Kenya has mostly been targeted by Al-Shabaab militia in a cyber warfare duel. Al-Shabaab is very active in the cyberspace recruiting more members and spreading their propaganda with an aim of influencing the minds if the unsuspecting youths. The militia group has been operating a number of websites spreading their radical ideologies and justifying attacks inside Kenya Somalia and the whole region. They also posts their written and audio messages in in their dubious websites after carrying out an attack. The problem is that there are no dedicated online counter terrorism teams that are willing to deter their webhosting activities. Twitter could be the only social media site that has consistently and actively prevented Al-Shabaab and other terrorist groups from misusing their platform to spread terrorism (Crisisgroup, 2015)

Anon_0x03 hacked and used Ruto's Twitter account to send abusive messages and publish a list of government Web sites it had defaced. The attack was apparently launched as "a cry for help" to expose corruption. Kenya was ranked one of the most corrupt countries in the world, at position 136 out of 177 by Transparency International. The hackers' campaign sent jitters across the country after the intruders penetrated Web sites with state secrets, and sensitive security and financial information. They included sites operated by the Central Bank of Kenya, Department of Immigration and Registration of Persons, the government's Integrated Financial Management Information System (IFMIS), Attorney General's office and Kenya Police Service.

Some of the Multinational companies that have suffered the sting of the hacktivists include Google Kenya, where the Web site, www.Google.co.ke, (was changed into a music site for hours in April 2013) commercial banks, telecommunication and media firms. While stating the reasons behind their campaign, a look at their posts on the affected sites gives clues about their motivations.

Impact of cyberwarfare in Kenya

FightingBack

The business level responses so far have seen Techno Brain, an IT solutions company, starting to offer hacking forensic courses to banks, government agencies and other corporates, while Kenya Methodist University (KeMU) launched a string of professional courses in IT security, in an attempt to plug some of the holes these attacks have highlighted. The government is moving in the right direction too. Kenya already set up their own Computer Incident Response Team (CIRT) to combat the problem, which aims to deal with incidents, promote security, issue warnings, and generally try to address the issues the country has with security and bring it up to scratch with the rest of the world.

Future

The future cyber warfare in Kenya, will need to be advanced to keep up with the growing technology. With the trends changing to convergence technologies such as big data, social media, embedded systems, mobility. The cyberwarfare will have to reach to newer heights, due to these trends. Besides the move towards Internet of things would possibly increase the crime rate in the cyberspace.

Conclusion

The African landscape is changing rapidly. This can be seen across expanding economies, rising populations and major technological developments. Over the last few years this has resulted in

many improvements. However, due to the pivotal nature of technology, one serious stumbling block to true progress could well be IT security.

References

Benyawa, L. (2016). *Agency says 3000 cyber-crime cases reported in Kenya monthly*. *Standard Digital News*. Retrieved 25 November 2016, from https://www.standardmedia.co.ke/business/article/2000204352/agency-says-3000-cyber-crime-cases-reported-in-kenya-monthly

CAK, C. (2016). *Communications Authority of Kenya*. *Ca.go.ke*. Retrieved 25 November 2016, from http://ca.go.ke/index.php/component/content/article/93-general/333-ca-to-receive-itu-technical-support-to-fight-cybercrime

Clarke, R. & Knake, R. (2010). *Cyber war* (1st ed.). New York: Ecco.

Claunch, C. (2014). *On cyberwarfare*. [Plaats van uitgave niet vastgesteld]: [uitgever niet vastgesteld].

Even, S. & Siman Ṭov, D. (2012). *Cyber warfare* (1st ed.). Tel Aviv: Institute for National Security Studies.

Gonzalez, M. (2015). International Perspectives of Cyber Warfare. *International Journal Of Cyber Warfare And Terrorism*, *5*(4), 59-68. http://dx.doi.org/10.4018/ijcwt.2015100103

Lepton, K. (2016). *Future Cyberwarfare Will Soon Overshadow Ground Wars | Future Technology 500*. *Futuretechnology500.com*. Retrieved 24 November 2016, from http://www.futuretechnology500.com/index.php/future-cyberwarfare/

Schreier, F. *On cyberwarfare* (1st ed.).

Shay, R. (2013). CyLab usable privacy and security laboratory. *XRDS: Crossroads, The ACM Magazine For Students*, *20*(1), 62. http://dx.doi.org/10.1145/2508976

IDG CONNECT,. (2016). *Cybercrime Hacking and Malware*. Retrieved from https://www.cylab.cmu.edu/files/pdfs/news/cybersecurityinthethreetimes.pdf

Serianu,. (2016). *Kenya Cybersecurity Report 2012*. Nairobi: Serianu. Retrieved from http://www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf

Andress J, W. (2011). *Cyber warfare:techniques,tactics and tools for security practitioners.* Elseiver Science.

crisisgroup. (2016, November 23). Retrieved from www.crisisgroup.org: http://www.crisisgroup.org/~/media/files/africa/horn-of-africa/kenya/b102-kenya-al-shabaab-closer-to-home.pdf

serianu. (2016, November 22). *www.serianu.com.* Retrieved from http://www.serianu.com/downloads/KenyaCyberSecurityReport2015.pdf