Nature of Cyber Crimes and Legislation in the Republic of Tunisia

Ahmed Ben Ayed

Abstract— The Internet has created unlimited opportunities for businesses as well as individuals. However, technology always has a destructive side as well as a beneficial side. In Tunisia, cyber security is becoming a threat to all sectors in the country. In order to protect the economy, the government has created new laws and legislations. This paper analyzes the cyber crime situation in the country and discusses the stance of the Tunisian government against cyber crimes, and the legislation in place to enforce the law.

***Index Terms*—Cyber Law, Cyber Crime, Tunisia, Hacktivism, Cyber Terrorism.**

I. Introduction

Cybercrime is known as the use of a computer to take, alter, or gain unlawful use of a system or computer [1]. Nowadays the Internet has created unlimited opportunities for businesses, and for individuals as well. However, the convenience associated with information technology and the Internet is now being exploited to serve criminal purposes [2]. Cybercrimes involve disruptions of network traffic - denial of service attacks/e-mail bombing, creation/distribution of viruses, identity theft, cyber stalking, cyber-squatting [3], pornography, extortion, fraud and impersonation [4]. Simply speaking, any unlawful act carried out on the Internet is considered a cybercrime [5]. According to the European council a cybercrime is “any criminal offence committed against or with the help of a computer network” [6].

II. Crimes and Cyber Crimes

The concept of crime is a behavior defined by the criminal law [7], and it is usually committed in a specific time and specific location. Cybercrimes are more complex and their range is extensive. The range and the variety of cybercrime make it very hard to come up to with a specific definition for it; different agencies and organizations have given different definitions according to their understanding or their environments. Some researchers define it as a crime that involves a network or a computer [8], others define it as a crime committed against or with the help of computer networks [6]. There are so many different forms of cybercrime that it is very difficult to cite them all since the technology is evolving so fast, and different techniques and methods are being invented every day.

III. Effect of Cyber Crimes

People and businesses around the world are being affected by cybercrimes. During 2012, 7% of people aged 16 or older were victims of identity theft, and about 14% of identity theft victims experienced out-of-pocket losses of $1 or more [9].

During 2013, the Internet Crime Report Centre reported that 262,813 reports were filed for an adjusted dollar loss of $781, which is a 48.8% increase in reported losses since 2012 [10]. Besides the economic effect, cybercrimes have some other effects that could be social, ethical or even terroristic in nature. Child pornography, for example, is one of the biggest concerns of Homeland Security in the United States; as reported in the Internet Watch Foundation’s annual report, about 58% of all known child abuse domains are housed in the United States [11]. Child pornography has become a $3 billion annual industry [12].

IV. Most-Used Cyber security Crimes in Tunisia

A. *Denial of Service Attack*

A denial of service attack is an attack on a computer system by a hacker or a virus that does not seek to break into the system or steal information; rather, it crashes the website by deluging it with phony traffic [13]. As of 2014, the frequency of recognized DDoS attacks had reached an average rate of 28 per hour [14]. If a website is a victim of a denial of service attack, information stored in the website is not going to be compromised as the attack does not go after information, it just makes the website and its services unavailable.

In the years following the Tunisian revolution (2011), the group Anonymous took a number of actions known initially as “Operation Tunisia” in support of the Tunisian activists. Anonymous launched a Distributed Denial of Service attack using hijacked servers as well as volunteers’ computers and attacked government websites. The website of the Prime Minister Mohamed el Ganouchi was also hijacked and videos and links were published on the website. Perhaps such attacks are preventable but difficult to pre-empt. Some firewalls do block traffic coming from the

***Manuscript received Feb, 2017*.**

***Ahmed Ben Ayed**, Department of Computer Science and Engineering, Colorado Technical University, Colorado Springs, Colorado, USA.*

same IP address if it seems to be non-legitimate traffic. However, hackers are also using new methods to change their IP address or to access servers anonymously. During 2010, pro WikiLeaks hackers brought down Tunisian government websites, including the personal website of the Tunisian president at that time Zine el-Abedine Ben Ali. The hacktivists were conducting their attack in response to the Tunisian government's block of websites that published WikiLeaks links. The following statement was released by the hackers: "The Tunisian government wants to control the present with falsehoods and misinformation in order to impose the future by keeping the truth hidden from its citizens. We will not remain silent while this happens. Anonymous has heard the claim for freedom of the Tunisian people. Anonymous is willing to help the Tunisian people in this fight against oppression. It will be done. It will be done." . . ."This is a warning to the Tunisian government: attacks at the freedom of speech and information of its citizens will not be tolerated. Any organization involved in censorship will be targeted and will not be released until the Tunisian government hears the claim for freedom to its people." [15].

B. Viruses

A virus is a program designed to infect and damage files on a computer that receives it [16]. The harmful code could be hidden in a file as a picture or a word document; as soon as the file is opened the code will be executed. The file also has the ability to reproduce itself. Antiviruses are the famous countermeasure for a virus. Most of the antiviruses use a signature database to detect viruses; however, this kind of technology is ineffective on fast-spreading viruses as well as custom-made ones. The antivirus relies on a database that contains all signatures of known viruses, which can be effective if the user is updating that database on a regular basis. Other detection techniques exist, such as behavioral detection techniques, but they cost more money and take a lot of resources, especially human resources.

C. Sniffing Attacks

Another type of attack is a sniffer attack, where an application or a device reads, monitors and records data traveling in the network. If the data is not encrypted, the sniffer will be able to obtain a full image of the data. Using a sniffer the attacker can analyze the data going in and out of the network as well as read all communications. If an encryption is used the attacker will need the key to decrypt the information. According to the National Security Agency, most hackers use sniffing techniques to get information that helps them to hijack victims' accounts.

D. Software Privacy or Copy Rights

The Business Software Alliance defined software piracy as the illegal copying, downloading, sharing, selling or installing of copyrighted software. Also according to the (BSA) Global Software Piracy Report, the rate of software piracy in 2009 was 43%- which is considered to be high- however, it is higher in third world countries because of the limited economic resources [17]. BSA confirmed as well that the software piracy rate in Tunisia is about 74%, which is considered to be seriously high compared to 27% in the United States for the same period [17].

E. Cyber Terrorism

Cyber terrorism does not have a specific definition; to date, the international community has not decided yet on an exact definition of terrorism or cyber terrorism that could be used internationally. The United States uses the following definition of terrorism: "premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents." [18]. Cyber terrorism is harder to define internationally than terrorism itself. According to NATO, cyber terrorism is "a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal."[19]. Another definition provided by the Department of Homeland Security is "a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies." [20].
When looking at all definitions we conclude that even scholars are divided and do not really have a specific definition for the matter. Stohl (2007), defined cyber terrorism as a "convergence of terrorism and cyberspace." Basically, the means and their application are the same as regular computer network attacks, with the significant difference being that in the case of cyber terrorism, the leading motive is to coerce the government or its citizens to comply with some political or social demands. Moreover, the act should result in violence or fear in order to be qualified as cyber terrorism. Minor attacks that disrupt services of no great importance are not cyber terrorist acts, yet they may prove a very expensive nuisance, in terms of economics [21]. Tunisia has not encountered any cyber terrorism acts to date; however, cyber terrorism threats are getting worse, especially as a lot of well-educated Tunisian youth are joining terrorist organizations in the region of the Middle East. Homeland Security Department has published some unclassified information about cyber terrorism groups that are trying to launch cyber-attacks against the United States and its allies' computer systems. The Department talked about an operation called "Operation Black Summer" (#OpBlackSummer) orchestrated by hacktivist groups Tunisian Cyber Army (TCA) and the Al Qaeda Electronic Cyber Army. The premise of the operation was to hack into varied U.S. systems, steal information, and release the information in a large data release on 11 September 2013 [22].

V. Legislation

A. The Tunisian Electronic Exchange and Electronic Commerce Law of 2000

Tunisia enacted its Electronic Exchanges and Electronic Commerce Law on August 9th, 2000. The objective of the law was to promote e-business and facilitate its growth via the creation of a legal framework. According to the law, an electronic document has the same legal validity as a physical written document. The e-document is applicable in all matters, the only requirement being a digital signature using a certified solution whose technical specifications are laid down by a decree from the minister of telecommunication. For a party to electronically sign any document, they must possess a pair of keys: a private one and the appropriate public one. The law recognizes foreign signatures as well, which makes the country very open to accepting international business. Tunisian law adopted a mandatory regulation over certification in order for authorities to better control and offer a high degree of security. Any individual or entity that is offering certification services has to be licensed; any illegal engagement in certification work is penalized with a jail term and a fine.

B. The Tunisian National e-Commerce Law of 2009

Tunisia has been experiencing a rapid growth in internet accessibility; however, the use is still not organized and beneficial. Over the past decade the developing country has succeeded in enacting its first national e-commerce law in 2000 for the purpose of achieving more security in e-commerce transactions and providing a legal groundwork for it.

C. The Tunisian National Cyber Criminal Law

After the Tunisian revolution many hacktivists conducted denial of service attacks and other attacks on government servers, and many videos considered offensive and violent were uploaded to the internet. It became urgent to draft a law to be able to enforce the removal of these and prosecute those involved. In 2014, the government adopted a new constitution that was “enshrining the rights to access communication networks, personal data protection, and freedom of expression,” as Reporters Without Borders claimed. As of today the Cyber Criminal Law still has not been passed, and it is has been prevented from being passed after the elections of November 2014. However, activists are claiming that the draft of the law is vague and not specific in language. One of the articles in the law proposes a six month prison term and fine for assaulting good morals [23]. The Tunisian government is showing some concerns about the rise of terrorism activities in the region, and so activists are afraid that the government may use the issue of terrorism to limit liberties. However, authorities are claiming that they are not going to engage in any online censorship activities.

VI. Conclusion

In the computer age, technology plays a primary role in conducting business transactions, and helping people learn and achieve their goals quickly. However, Cyber crimes are jeopardizing many sectors, and primarily affecting business and e-government services.

This paper begins with an explanation of what is meant by cyber-crime in order to give an understanding of the topic in the context of Tunisia. The unique problems in the arena of cyber-crime faced by the country are then addressed, followed by what steps the Tunisian government has taken to fix these problems.

References

[1]. Jewkes, Y., & Yar, M. (2013). Handbook of Internet crime. Routledge.

[2]. Ayantokun, O. (2006). Fighting cyber crime in Nigeria. *Info secs News www.networksecurityarchive. org/html/Information-Security-News/2006-07/msg00021. html (accessed Nov., 2010).*

[3]. USA Information Resources Management Association. (2011). Cyber Crime: Concepts, Methodologies, Tools and Applications. IGI Global.

[4]. Awe, J. (2004). Fighting cyber crime in Nigeria. *Retrieved from http://www.jidaw.com/itsolutions/security3.html.*

[5]. Pas, P. (2007). Cyber crime: hardships to curb it. *Retrieved from www.naavi.org/pati/cyber_crimes1.html*

[6]. European Union (2001). The Convention on Cyber-Crime, a unique instrument for international co-operation. *Retrieved from http://www.europarl.europa.eu/meetdocs/2014_2019/documents /libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf*

[7]. Cressey, D. R. (1951). Criminological research and the definition of crimes. *American Journal of Sociology, 56*(6), 546-551.

[8]. Kowalski, M. (2002). Cyber Crime: Issues, Data Sources and Feasibility of Collecting Police-Reported Statistics. Ottawa: Canadian Centre for Justice Statistics.

[9]. Harrell, E., & Langton, L. (2013). Victims of identity theft, 2012. *Washington DC: Bureau of Justice Statistics, 26*.

[10]. FBI (2013). 2013 Internet Crime Report. *Retrieved from* http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf.

[11]. Smith, S. (2014). Preliminary Analysis of New Commercial CSAM Website Accepting Payment by Bitcoin. Internet Watch Foundation.

[12]. Grubbs, J. B., Exline, J. J., Pargament, K. I., Volk, F., & Lindberg, M. J. (2016). Internet pornography use, perceived addiction, and religious/spiritual struggles. *Archives of Sexual Behavior*, 1-13. Watch Foundation.

[13]. Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2016). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Communications Surveys & Tutorials, 18*(1), 602-622.

[14]. Preimesberger, C. (2014). DDoS attack volume escalates as new methods emerge. *Eweek*.

[15]. Hussain, M. M. (2016). *State power 2.0: Authoritarian entrenchment and political engagement worldwide*. Routledge.

[16]. Cohen, F. (1987). Computer viruses: theory and experiments. *Computers & security*, *6*(1), 22-35.

[17]. BSA. (2012). Shadow Market: 2011 BSA Global Software Privacy Study. K. I., Volk, F., & Lindberg, M. J. (2016). Internet pornography use, perceived addiction, and religious/spiritual struggles. *Archives of Sexual Behavior*, 1-13. Watch Foundation.

[18]. Ruby, C. L. (2002). The definition of terrorism. *Analyses of social issues and public policy*, *2*(1), 9-14.

[19]. Everard, P. (2008). Nato and Cyber Terrorism. *Centre of Excellence Defence Against Terrorism*. IOS Press.

[20]. Wilson, C. (2003). Computer attack and cyber terrorism: vulnerabilities and policy issues for congress. *Focus on Terrorism, 9,* 1-42.

[21]. Stohl, M. (2006). Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? *Crime, law and social change, 46*(4-5), 223-238.

[22]. Richard. B, (2013). Cyber Strategies & Resources for Resiliency Spring Directors Conference 2013. *Retrieved from http://ema.ohio.gov/Documents/DirectorsConference/2013_PPTs/Director%20Rick%20Baron_CyberEMAConference_2013.PPTX*

[23]. Mortiz, C. (2014). Tunisia cyber-crime law threatens Internet progress. *Retrieved from* http://vpncreative.net/2014/07/30/tunisia-cyber-crime-law-threatens-internet/

Ahmed Ben Ayed has received his Bachelor of Science in Computer Information Systems, Master of Science in Cyber Security and Information Assurance, and currently pursuing a doctorate degree in Computer Science at Colorado Technical University, his research interest are Android Security, Pattern Recognition of Malicious Applications, Machine Learning, Cryptography, Information & System Security, and Cyber Security.