"Dimitrie Cantemir" Christian University
Knowledge Horizons - Economics
Volume 11, No. 1, pp. 93 – 98
P-ISSN: 2069-0932, E-ISSN: 2066-1061
© 2019 Pro Universitaria
www.orizonturi.ucdc.ro

COMPARATIVE STUDY ON CYBERTERRORISM IN EAST ASIA AND NORTH AFRICA

Florentina-Stefania NEAGU[1], Anca SAVU[2]

[1] *Bucharest University of Economic Studies, Romania, E-mail: stefanianeagu15@yahoo.com*
[2] *National Defence University "Carol I", Bucharest, Romania, E-mail: ancasavu91@yahoo.com*

Abstract *The two regions resemble the fact that both are threatened by non-state entities, hacker attacks target institutions and companies, in order to influence a political decision or to obtain money by decrypting the data. In East Asia, China and South Korea have well-established legislation on cyber security, and with regard to North Africa, regional and continental leadership is Egypt that has developed cyber-incidence prevention systems in recent years and is also a cyber security provider at the region level. Over the past two years, cyber threats have grown globally, affecting shipping, air transportation, production lines and critical infrastructure.*

Key words:
Cyberterrorism, hackers, legislation, malware, nuclear threat
JEL Codes:
F5, F52

1. INTRODUCTION

Cyber threats pose a great risk to any company or state on the globe. Currently, only six countries have implemented the best cyber security measures, these are the United States, Russia, Israel, Spain, Estonia and China. Other states that follow the example of the six countries mentioned are Canada, Great Britain, France, Sweden and Malaysia (Analytics Insight, March 2019).

In 2017, China passed another law on cyber security to strengthen national security (Analytics Insight, February 2019). This change in cyber security law comes amid the evolution of systems based on artificial intelligence that are able to learn and develop their own server breakdown algorithms or threat detection for which they have been programmed but also the fact that the Chinese state is one of the five major states (Singapore, Malaysia, the United States of America and the United Arab Emirates) that have adopted facial recognition technology.

Currently, China has about 170 million surveillance cameras, and in the next three years they are expected to reach 500 million (Dialani, 2019). Moreover, the Chinese government announced that 60 airports are equipped with facial recognition systems, which leads us to the conclusion that the more a state is technologically more dependent and dependent on this technology, the higher the vulnerability to attacks from third parties.

2. TACTICS USED BY HACKERS IN THE TWO REGIONS

Hackers are constantly using new strategies to get e-mail security gateways, and brand impersonation is used in 83% of phishing

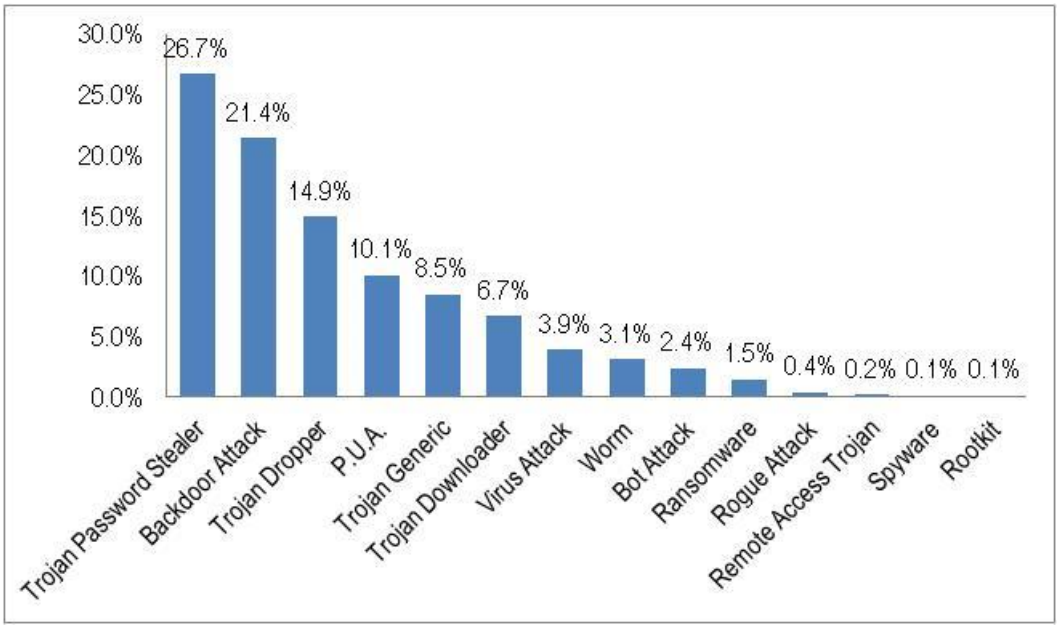
attacks, while one in three email compromises are launched through accounts Gmail. A common form of blackmail is represented by scams, which represent 10% of all phishing attacks. Multinational employees are twice as likely to be the target of this type of blackmail.

US Company Barracuda has made a report analyzing more than 300,000 emails, identifying three major types of attacks: brand impersonation that involves creating an email or social media account by assuming the identity of a known company, compromising the email addresses of companies and blackmail.

These attacks are popular and are constantly evolving, those who use them are constantly diversifying their tactics to avoid detection by target companies or authorities. Creating Microsoft's fake accounts is one of the most common techniques used by hackers to take control of official email addresses. This tactic has a high level of success especially for those who read their service emails on the phone (Help Net Security, 2019).

As can be seen in Figure 1, the types of malware used by hackers are very diverse and very difficult to combat.

Figure 1. **Types of malware used on companies in both regions**



Source: Author's own processing based on Comodo Report

Cyber space is an attractive environment for the new generation of terrorists, due to anonymity, psychological impact and its potential to cause massive damage. Numerous studies have been carried out by researchers from Europe, the Middle East and North America on analyzing illicit activities and cyber terrorism. However, there are limited studies on regions such as Southeast Asia, East Asia. Southeast Asia faces very real threats from the Islamic State. Fears are on the rise because Southeast Asia is hosting booming economies and a growing number of people adopting digital

technology, making them vulnerable to cyber attackers. Prime Minister Lee Hsien Loong predicted the opening of the Southeast Asian Nations Association (ASEAN) summit in Singapore that digitization has made the countries more vulnerable to cyber attacks (Law, 2018).

Governments in the Asia Pacific region are strengthening their cyber weapons in the fight against the Chinese cyber war targeting their countries. According to FireEye, the number of Asia-Pacific countries that have adopted offensive cyber skills has risen from four - China, North Korea, Pakistan and India to at least 14.

Experts say China has seen a sharp increase in cyber attacks across the region in the past two years, partly as a result of the Beijing 2015 negotiations with the US to refrain from cyber-spying. After signing this agreement, China has redirected its attention to Asia, according to Samm Sacks, a computer science specialist in China, at the Center for Strategic and International Studies. But the US trade representation said Beijing is not respecting the 2015 agreement, with espionage over the US being bigger than during the Cold War.

As regional countries have modernized, they have increasingly relied on web-based technologies to enable them to use their resources more efficiently. This virtual process reflected the uneven pattern of economic development found in East Asia. Countries such as Japan, South Korea and Singapore are more technologically advanced than other countries such as China, Indonesia, Malaysia, the Philippines and Thailand, but even more advanced than countries such as Brunei, Cambodia, Laos , Myanmar or Vietnam (Korean National Police Agency, 2008). However, the infrastructure of all other except the first set of regional countries is rudimentary compared to more developed countries in Europe and North America.

The need to respond to this security challenge can be seen in increasing the exposure of East Asian network users to cyber attacks. In Japan, for example, the number of cybercrime discovered by the police in 2004 increased by 13% from the previous year. A similar trend is also found in South Korea, where identity fraud and hacking are the most common cybercrime techniques (Stone, 2005). In addition to this, the nature of threats is also much more sophisticated. These range from scamming pshishing scams to spam, viruses and other malware that allows offenders to take remote control, for example, China, ranked second after the US in terms of its forms of activity malicious behavior (Symantec, 2007).

For some, such as Japan or South Korea, Internet connections are common and there is a rapid adaptation to new technologies. In other countries like Laos or Vietnam, the presence of the Internet is very limited. Differences in Internet connectivity have a direct correlation with the state's economy, with its modernization and integration into global development processes. These factors have a direct effect on the types of cyber security challenges. These differences form the approaches of East Asian countries to cyber security issues.

In Table 1 are shown laws governing on cyber terrorism and cyber crime in East Asia.

***Table* 1. Cyber Legislation in East Asia**

	East Asia					
	China	**Taiwan**	**Japan**	**Mongolia**	**North Korea**	**South Korea**
Legislation on Cyber Security	Cyber Security Basic Law of the People's Republic of China 1-Jun-17	Information and Communication Security Management Act 6-Jun-18	Basic Cybersecurity Act, 12-Nov-14	Draft of *Cyber Security ACT* 2013	-	*National Cyber Security Management Regulation*
Global Cybersecurity Index/Rank 154 Countries	32	-	11	104	52	13
Nuclear Threat Index	26	32	4	49	24	17
Nuclear power	45 in operation 15 under construction	4	37	-	-	23

Source: Author's own processing

A common element with regard to the two regions is given by cyber threats. At the level of the region one of the challenges is the implementation of cyber-terrorism laws.

Egypt adopted a bill on cyber-threat, at the end of 2014, set up a Cyber Security Council with the aim of creating a national strategy to ensure government agencies' infrastructure and networks against cyber attacks and personal education Government to prevent computer intrusions on institutional email addresses. According to statements by the Egyptian Minister of Communications and Information Technology, hackers do not have a specific profile but have different objectives, noting that many organized crime groups are trying to sabotage Egyptian financial systems. At the level of the African continent, Egypt continues to take steps to prepare other states to improve their cyber defense capabilities (Unipath, 2015).

Annually, The Economist and Intelligence Unit calculates the Nuclear Threat Index to identify vulnerabilities of nuclear installations to computer intrusions and responsiveness to sabotage as well as radioactive material transport security. The index indicates that Egypt is close to the bottom of the plant's ranking, ranking 43rd out of the 153 countries surveyed. It underlines that the country's nuclear safety situation could be improved by introducing stricter laws and regulations on physical physical protection systems, implementing effective response capabilities, addressing internal threats, and providing a cyber security system to nuclear installations.

Tabel 2. **Cyber Legislation in North Africa**

North Africa					
	Algeria	**Egypt**	**Libya**	**Morocco**	**Tunisia**
Legislation on Cyber Security	Penal Code; Law for Post and Telecommunications; Law to Prevent and Combat ICT Cybercrime	Cyber Crime Law June 5,2018	-	National Cyber Security Strategy Dec-12	Criminal Code; The Telecommunication Code; Circular no 19 dated April 11, 2007 regarding reinforcement of cybersecurity measures in public institutions
Global Cybersecurity Index Rank/154 countries	68	14	105	49	40
Nuclear Threat Index	42	43	112	37	30
Nuclear power	1	1	1	1	1

Source: Author's own processing

As can be seen in Table 2, Algeria ranked 42th in the ranking and its conditions could be similarly improved by implementing strong laws and regulations to address internal threats, improving intervention systems in situations of urgency and better security in cyberspace. Maroc is ranked on 37 with the possibility to improve its nuclear safety conditions, taking into account the potential levels of the radiological consequences of sabotage when developing protection measures, additional controls and limits for access to vital areas, measures to mitigate internal threats, implementation to respond to incidents of nuclear installations.

Cyber attacks on nuclear power plants pose a threat to any state, the explanation derives from the fact that taking over control of the plants and their use for criminal purposes can cause a tragedy among the population, secondly, some countries export raw materials produced by the power plants and the diversion of these materials can cause economic losses.

CONCLUSIONS

The two region there are several groups of hackers, and in most cases attacks have motivation monetary order. Types of attacks targeting companies are trojan password steal, backdoor attack, trojan dooper and others. This hostile activity against companies has led governments to adopt new laws or to propose draft laws to be adopted later.

The vulnerabilities in communications systems are also due to the fact that some of the

states have delayed the implementation of cyber security legislation for a long time, but also the fact that they are often unable to detect cyber intrusions, reacting after the incident .

REFERENCES

- Analytics Insight. (February 18, 2019) ,,Top 6 Countries with the Best Cyber Security Measures", available on-line at https://www.analyticsinsight.net/top-6-countries-with-the-best-cyber-security-measures/ , accessed at March 27, 2019
- Analytics Insight. (March 17, 2019) ,,How Disruptive Technologies are Transforming the Cyber Security Landscape", available on-line at https://www.analyticsinsight.net/how-disruptive-technologies-are-transforming-the-cyber-security-landscape/ , accessed at March 28, 2019
- Comodo (2018) ,,Global Threat Report 2018 Q 3", Clifton, United States, available on-line at https://www.comodo.com/GTR/Q3/2018/Comodo-Cybersecurity-Global-Threat-Report-Q3-2018.pdf , accessed at March 24, 2019
- Dialani, P., (January 24, 2019). Top 5 Countries to Adopt Facial Recognition Technology, available on-line at https://www.analyticsinsight.net/top-5-countries-to-adopt-facial-recognition-technology/, accessed at March 24, 2019
- Getting the Deal Through (February 2019) ,,Cybersecurity Japan", available on-line at https://gettingthedealthrough.com/area/72/jurisdiction/36/cybersecurity-japan/, accessed at March 25, 2019
- International Telecommunication Union (2018) ,,Global CyberSecurity Index 2018", available on-line at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, accessed at March 26, 2019
- Help Net Security (March 21, 2019) ,,Latest tactics used by cybercriminals to bypass traditional email security", available on-line at https://www.helpnetsecurity.com/2019/03/21/bypass-traditional-email-security/, accessed at March 25, 2019