International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Cyberwar Preparedness

Mamady Aissata Conde[1], Jamaludin Ibrahim[2]

International Islamic University Malaysia Jalan Gombak, 53100 Kuala Lumpur, Malaysia

Abstract: ***Cybercrime has increased considerably in the digital world. This harmful phenomenon, which is none other than cyber-attacks, cyber threats, cyber wars, cyber threats, etc., pose enough problems for the security of States, organizations, individuals and, above all, the digital economy. This paper provides a broad knowledge of cyber warfare, cyber-attack, cyber threat, threat categories, and their nature to provide data on preventive methods for cybersecurity, and offensive methods in cyberspace.***

Keywords: Cybersecurity, cyberwar, cyber-attacks, cyber threat, cyber Offensive-defensive, preventive approach

1. Introduction

The field of cybersecurity is very broad and complex and deserves a lot of thought and analysis to protect the digital world. The world is making great strides towards ICTs, which are making significant progress in social and economic development. Private and public companies, as well as individuals, have integrated information and communication technologies into their daily lives. Mobile telephony and other services offered on smartphones are gradually taking the lead in terms of means of communication and access to information.

Cyber-attacks are a difficult phenomenon to grasp and often important. They come from an organized group or an isolated person, it is a fraudulent act against a computer system, which is justified by political and economic claims. Therefore, in recent years, we have been confronted with the rise of cyber-infractions that effect, to varying degrees, the entire sector. Whether it is incivility, harassment, espionage, dysfunction, fraud, theft, destruction, surveillance, activism or even terrorism or misinformation, any form of crime, violence or conflict takes place over the Internet[1].

Indeed, to have an expected result, confidence in digital must be ensured. The availability, integrity, confidentiality and sensitive information used, stored and transmitted must be guaranteed. These are the challenges of cybersecurity. But this information is threatened by repeated cyber-attacks from cyberspace. Risk reduction has, therefore, become an issue that inevitably concerns countries, organizations, and citizens[2].

The virtual space created by interconnected computers and computer networks on the Internet. Cyberspace is a conceptual electronic space unbounded by distance or other physical limitations. William Gibson coined the term in his novel Neuromancer (1982) to describe an advanced virtual reality network. See also Internet and virtual.

Ensuring cybersecurity in a country also means understanding the challenges and consequences of digital developments in the military, defense and military sectors. Cyberspace is now considered the fifth battlefield. It is an area of military operations in the same way as land, sea, air, and space[3].

Understanding the dangers to which the individual is exposed, the public and private organization, the State and, more generally, society, can act. In order not to stand idly by in the face of the dangers of cyber-attacks or technology piracy, political and economic leaders must understand the fundamentals of cybersecurity necessary to control risks and ensure the harmonious development of the digital ecosystem[3].

This describes a risk optimization strategy for thinking about cyber-attacks, determining a good strategy to reduce risk, plan, and promoting a good defensive and offensive method.

2. Literature Review

The Internet communicates virtually with everyone, and therefore with anyone. It is complicated, if not impossible, to verify who is behind a screen, remotely or behind a virtual identity, fake identity or pseudonym. There is no "security" mechanism that guarantees the good faith of Internet users, not to mention the robot software that feeds communication platforms. As expressed by[4] since innovation is produced with unimaginable speed, it turns out that it is part of our daily lives and has a positive or negative impact. Most would agree that the web turned into a focal factor of these innovative improvements.

The cyberspace with which we collaborate can be considered a common global space whose borders would be linked to the geographical location of the individuals who use it and the location of the physical support infrastructure. Global regulation of space could also frame cyberspace, as it would compromise the stability of countries, as cyberspace is only an economic and military battleground, characterized by all kinds of economic, political and technological conflicts or competitions. According to [5] Cyberspace security threats have become a major risk to national security; as President Xi Jinping stated, ‘‘It is impossible to ensure national security without the security of cyberspace. ”. As reported by [6] and Cyberspace has become the new battlespace where the weapons are social engineering, upgraded viruses, Trojan horses, worms, flooding Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS) or botnets, and advanced persistent threat (APTs).

Cyberspace is considered by some authors as a mathematical problem, which could be modelized to have a broad meaning to find an adequate solution to solve the equation of the

cyberspace security model. According to by [7] It is interesting to solve the equation of the cyberspace security model in recent scientific calculations and applications, such as the division of the microcontroller float. For example, we used Taylor expansions and infinite approximation thinking to obtain the root of the equation of the cyberspace security model. In addition, others have modeled game theory, which is a mathematical model of algorithmic optimization and analysis that will examine the number of threats to find strategies necessary to effectively solve cybersecurity and planning problems. Reporting by [8] Game theory captures the contradictory nature of cybersecurity interactions and provides quantitative and analytical tools that help to find optimal defense strategies. It will also allow us to examine many threat scenarios, thus, to predict the actor's behavior in uncertain situations and suggest probable actions and expected results.

Several authors havementioned the risks of cyber-attacks that leave no one indifferentbecause technology has become an integral part of us. This riskis divided into three parts: individuals, the organization and the state. Some of the main impacts of cyber risks on people may include defamation, intimidation, harassment, exposure to malicious content, misinformation and manipulation.Moreover, there is an impact of cyber risks in public or private organizations and the state, which can include imagereputation, industrial and economic espionage, competitive attacks, national security issues, and many others[9][10][11].

Regardless of your status, as soon as you use the Internet, you are exposed to cybersecurity risks. Therefore, protecting executives, systems, information, networks, and data in cyberspace from cyber threats or attacks requires some form of security. All technical means, strategies, methods, advice, activities, tools, processes, organizational, human resources and controls designed to protect, guarantee the security of your information, and defend the assets and privacy of users, organizations, agencies, and governments are called Cybersecurity[12][13][14].

Cyber-attacks and cybersecurity breaches have become an increasingly frequent activity among cyber attackers and have a major impact on governments and private entities, as well as individuals. These cybercrimes and major offenses have encouraged governments around the world to consider and improve the most effective methods of preventing, detecting and responding to these incidents. Mentioned by[15], the concept of cybersecurity focuses on protecting computers, networks, programs, and data from negligence and counteracts any unintentional or unauthorized access, modification or destruction.

Preparations for cyber warfare have become a necessary element in the construction of the army in several countries. The subject of cyberwar concerns the populations of all countries and not only politicians, army and diplomats. In addition, nation-states, non-governmental organizations, or individuals have taken advantage of the vulnerability and inter-connectivity of cyberspace to inflict enormous damage on countries and societies. When we examine the meaning of cyber warfare, it is a technological attack massively coordinated against a state by another state or non-governmental organizations to be able to penetrate computer systems and networks[13]. According to[16], the concept of cyber warfare can also be used to define attacks between companies, terrorist organizations or simply attacks by individuals called pirates, who are perceived as belligerents in their intent.

However, each State must respond to the need for global management and control of digital security and cyber-defense with the ultimate objective of controlling its advanced foundations, ensuring its quality, economy and population and monitoring digital threats at a satisfactory level[17].The government is well positioned to take a leadership role in exploring new technologies that will better protect our own systems, help industry focus more on supply chain security, protect the software ecosystem and automate the protection of citizens using the Internet in their dealings with government[16]. In addition, a national defense force, its army, must have a high level of technical knowledge to ensure the security of its IT and telecommunications infrastructures, in the same way as any other critical infrastructure[17].

In short, an operational army must be ready in terms of cyber defense, to defend its country, its population, and its economy in the event of an attack. And to have offensive countermeasures in case of an attack in order to defend territorial integrity[18].

3. Discussion and Analysis

How can we defend ourselves against cyber-attacks in cyberspace if we do not know enough about the phenomena and their modes of attack? The information sources and strategic systems maintained on these networks are potentially lucrative targets for terrorists, foreign governments, criminal organizations, and competitive businesses. The organization must be able to understand the nature of cyber threats, their evolution, and impact. To prepare for attacks, it is recommended to identify the organization's confidential information to set up a more efficient monitoring system and make optimal use of the resources deployed[19]. In this article, we will discuss the different categories of cyber threats that have been mentioned by scientists. Technology, like all sciences, has both positive and negative characteristics. Preparing for cyber-attacks is therefore essential, if not mandatory, to protect technology logistics from these threats. The major event of the cyberwar could depend on four main factors: (1) the type of threat, (2) the severity of the threat, (3) the attribution sensitivities and (4) the identity of the cyber-attacker[20].

According to control system security expert Eric Byres of Belden Inc. and Tofino Security, about 50% of cyber-attacks that enter the control network system come from the company's system, 17% from the Internet, and 10% from trusted third parties [21].

4. Cyber Threats

Cyber threats are generally intentional actions or accidents that can disrupt the proper functioning of a computer system

or network. These threats can be internal to the company by members or external. [21].

1) Internal threats

Internal threats can come from dissatisfied employees of the company, but not only from them. They may also be carried out by current or former subcontractors, business partners, who have or have had authorized access to an organization's network, system or data and who have deliberately exceeded or used such access in a manner that has compromised the confidentiality, integrity or availability of computer systems [21]. Historically, employees have been the greatest risk. They have knowledge, authorizations and time in their favor. For example, the data leak may be intentional. An employee saves critical information on a USB stick, or sends it to his personal email, then sells it to the competition. This data leak may also be due to the negligence of employees who browse unsecured sites or leave their session open or use passwords that are too low[22].

Figure 1.1: Internal Threats [tech crunch 2018]

2) External threats

External cyber threats are malicious attacks that come from outside, mainly from the environment in which the company operates or from a distance. Threat actors, hackers and attackers attempt to exploit security risks within the perimeter of your attack surface. These include threats to network protection, physical threats, piracy threats, software threats, socio-economic and legal threats. All organizations with a digital presence are exposed to external threats from attackers. The most frightening attacks come from skilled and sophisticated external hackers. These attackers may find network vulnerabilities or socially manipulate insiders to bypass the network's external defenses. Attacks are generally aimed at damaging the image of their target, paralyzing or holding them to ransom. The attacker exploits the system's securityweaknesses[21][22].

Figure 1.2: int [Francophonie 2016]

How Attackers can gain access to the control Network

Hackers seeking to penetrate computer systems first analyze vulnerabilities, i.e., failures that affect the security of a company's system, protocols, operating systems, applications or even personnel. To implement an exploit, the first step of the hacker is to collect as much information as possible about how the network works, the operating systems and the applications on it. Most attacks are the work of script kiddies who foolishly attempt to hack into the Internet, without any knowledge of the system or the risks associated with their actions. The hacker, once he has mapped the system, is able to implement attacks related to the versions of the applications he or she has detected. Initial access to a machine will allow it to extend its action to retrieve other information, and if necessary, to extend its privileges on the machine. When administrator access is obtained, it compromises system files. The pirate then has the highest rights on the machine. The last step consists in erasing its traces, to avoid any suspicion on the part of the administrator of the compromised network and to be able to keep control of the machines concerned for as long as possible[21][22].

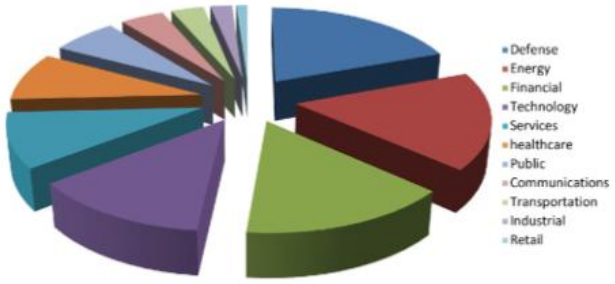

Figure 2: Cybercrime activity [Robert, Shimonski 2014]

5. Common threats to be Aware

Each country is currently facing cyber threats from state and non-state actors that can affect its security, integrity, and stability. Computer threats are varied and very effective. We present below some of the different forms of attacks:

- **Botnet**

The word Botnet is made up of the word's "robot" and "network". A botnet is a network of pirated computers under the control of illegitimate actors. Cybercriminals use special Trojan viruses to compromise the security of multiple users' computers, take control of each computer and group all infected machines into a network of robots that the criminal can remotely manage using command and control software.

They include:

- Web application attacks to steal data
- Send spam with viruses as attachments.
- Spread all malicious software.
- Can use your computer for a denial of service attack against another system.

Figure 3: Vicious cycle between spam and cybersecurity [ITU-D 2017]

- **Distributed denial of service (DDoS)**

Denial of service attacks is caused by the flooding of a server or website with requests to make it inaccessible. Denial of service attacks can be carried out by a small number of people. A cyber-pirate can use his only computer to control zombies, that is, other infected computers that obey his orders. These computers may have already been infected by viruses or worms.

- **Pharming**

Pharming is a commonly used type of online fraud. Pharming redirects Internet users from authentic websites to fraudulent sites using a strategy called DNS Cache Poisoning, where data is corrupted and inserted into a DNS cache database. The attacker applies several attack methods, but the most common is to modify the host file. The hacker hides behind the target's computer and takes him to a fake website. The objective is to recover confidential information such as credit card numbers, account passwords, etc.

- **Phishing**

Phishing remains one of the main factors in cybercrime. This type of attack involves obtaining from the recipient of an apparently legal email, the transmission of bank information or financial services login credentials to steal money. Phishing can also be used in more specific attacks to try to obtain an employee's access information to the professional networks they can access.

- **Ransomware**

Ransom-software is one of the most widespread viruses currently available. This consists of sending the victim malware that encrypts all his data while blocking all files on the computer and asking him for a ransom in exchange for the decryption password.

6. Preventive Approach

But we note that, very generally, companies are behind in the implementation of the cybersecurity program. This is due to three aspects: lack of adaptation, they take too long to cope with change and adapt; lack of budget, usually the budget allocated to cybersecurity in companies is not significant; and finally, the lack of skills, the lack of cybercrime specialists in companies is a problem.

Faced with such IT threats, it is necessary to apply a security and prevention policy based on three axes: employee training, strengthening protection barriers and data backup. But IT security is a complex issue. Being supported by experts allows you to benefit from specialized skills and solutions adapted to your needs in a field that is constantly evolving in terms of risks and protection.

In short, we recommend that companies invest in security, have a security operations center (SOC) that will oversee and manage information security, create a dedicated cybersecurity team that focuses on training, qualification to ensure that IT security is integrated on a daily basis, create a rapid detection system, familiarize themselves with electronic threats and their consequences, and be proactive. To protect against attacks, it is recommended to identify the organization's sensitive information to set up a more relevant monitoring system and make better use of the resources implemented.

Offensive and Defensive Preparation For Cyber Warfare

All countries must adopt a strategy and operational measures that will enable them not only to develop the robustness and resilience of their digital infrastructures, but also to demonstrate their cyber defense and cyber-determination capabilities in order to contribute to international peace and stability, conflict prevention and the protection of populations, the integrity of cyber territories and assets and their values.

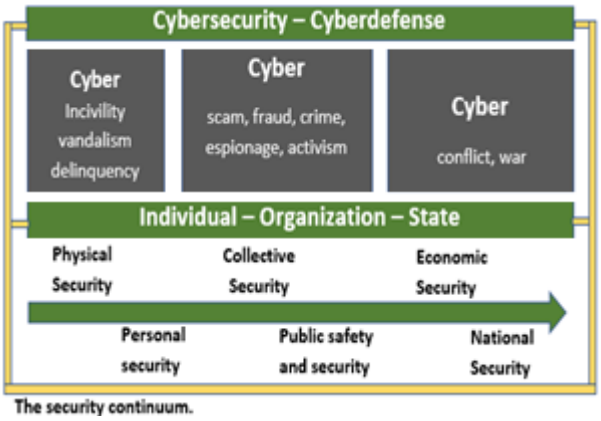

Figure 4: The security continuum [Francophonie 2016]

Cyber Offensive

In cyber warfare, countries must be much better prepared for the offensive attack, as they are inexpensive and have a high yield for the attack. For example, if the attacker and defender have the same resources, the attacker will win. The 2007 cyber-attacks against Estonia did not cost the attackers much, but they had significant repercussions in terms of disruption for the Estonian government[23]. The effectiveness of traditional defenses now depends on IT capabilities. A country's cyber offensive is the way to project its power, by deploying technological forces beyond its geographical borders. Thus, computer code and programs are electronic fighters, remotely controllable, allowing the enemy to be forced by cyber-attacks and to intervene in foreign cyber territories without being officially declared war on opponents targeted by offensive computer acts[22].

Cyber defensive

Cyber defense is a key area of security. Its role is to control all the technological infrastructures of a country. According to by[23]Defense is said to be superior if the resources required to capture the territory are greater than the value of the territory itself. To deal with cyber-attacks, it is necessary to demonstrate organization, preparation, tools, skills, know-how, processes, as well as training and simulation exercises in crisis management and on interventions in cyber-attacks. It also requires a political vision, a national cybersecurity strategy that translates into the effectiveness and operational efficiency[22]. Civilian-military actors must be introduced to cybersecurity and cyber-defense for a complete knowledge of systems, vulnerabilities, attention, intelligence function, active and dynamic supervision of the context of cyber-attacks.

7. Conclusion

Cybercriminals exploit all technological advances. Their methods and techniques are increasingly sophisticated and difficult to combat. Companies will face new types of attacks, and it is essential to put in place the right foundation for dynamic, not static, defense to protect themselves. In addition, work with all the stakeholders that make up the organization's ecosystem (all members) to protect information. Secondly, States must invest in cyber-protection, assistance to civil authorities, intelligence, cyber-offensive, cyber-offensive, passive and active cyber-defense as well as missions, the roles of the army must be clearly defined and taken into account in a cyber defense strategy to provide the means necessary for effective governance and the realization of cyber defense.

8. Summary of Literature Review

Author	Contribution	Result	Limitation
K. Pipyros et al, 2016	Presents major cyber-attack incidents and their impact on the States. Examines the existing legal framework at the European and international levels. Approaches "cyber warfare" from the perspective of international law and focuses on two major issues relating to cyber operations, i.e. "jurisdiction" and "attribution".	Identified the technical, legal and political difficulties. Emphasize the complexity in applying international law rules in cyber operations	Very few evidence wer presented. More evidence is required
Abderrah mane Sokri, 2018	Explores the main open issues in the application of security games in cyberspace. Novel game formulation that has simulation and game-theoretic approaches is proposed and illustrated	Assumed in these games that the defender knows his own payoffs and the payoffs of the follower. The follower is also assumed to know his own payoffs and the strategy to which the leader committed to.	Did not explore possib extensions of this framework to other rea world situation such as A dynamic formulatio of the problem where recent attacks are built upon previous attacks
Xiao-NiuYang et al, 2018	Presents the tripartite theory of cyberspace, based on the status quo of cyberspace. Corresponding strategies and a research architecture are proposed for common public networks (C space), secure classified networks (S space), and key infrastructure networks (K space), based on their	Introduce the SMCRC (which stands for "situation awareness, monitoring and management, cooperative defense, response and recovery, and counter measures and trace back") loop for constructing a cyberspace security	Pointed that humans have created cyberspac we should also take responsibility to make a healthy, orderly, and autonomous ecosystem

References

[1] P. J. Ortmeier, *Introduction to security*: Pearson, 2017.
[2] C. Johnson, L. Badger, D. Waltermire, J. Snyder, and C. Skorupka, "Guide to cyber threat information sharing," *NIST special publication*, vol. 800, p. 150, 2016.
[3] R. Shimonski, *Cyber reconnaissance, surveillance, and defense*: Syngress, 2014.
[4] R. Litwak and M. King, "Arms Control in Cyberspace?," *Wilson Briefs,(October 2015). https://www. wilsoncenter. org/publication/arms-control-cyberspace*, 2015.
[5] X.-N. Yang, W. Wang, X.-F. Xu, G.-R. Pang, and C.-L. Zhang, "Research on the Construction of a Novel Cyberspace Security Ecosystem," *Engineering*, vol. 4, pp. 47-52, 2018.
[6] A. Sokri, "Optimal Resource Allocation in Cyber-Security: A Game Theoretic Approach," *Procedia computer science*, vol. 134, pp. 283-288, 2018.
[7] Q. Yong, L. Qianmu, and H. Jun, "A Method to Solving Cyberspace Security-model Equation," *Procedia Engineering*, vol. 15, pp. 2052-2056, 2011.
[8] A. Sinha, T. H. Nguyen, D. Kar, M. Brown, M. Tambe, and A. X. Jiang, "From physical security to cybersecurity," *Journal of Cybersecurity*, vol. 1, pp. 19-35, 2015.
[9] K. Pipyros, L. Mitrou, D. Gritzalis, and T. Apostolopoulos, "Cyberoperations and international humanitarian law: A review of obstacles in applying international law rules in cyber warfare," *Information & Computer Security*, vol. 24, pp. 38-52, 2016.
[10] M. I. Marinescu, "Cyberwar & cyberterrorism heading towards a cyber-waterloo," *Annals of the University of Oradea*, vol. 7, pp. 49-60, 2015.
[11] M. A. Ammar, L. A. Ismail, Z. Zakaria, and J. Ibrahim, "Cyberwar Preparedness," *International Journal of Information and Communication Technology Research*, vol. 6, 2016.
[12] S. S. Administration, *Social security programs throughout the world: Asia and the Pacific, 2012*: Government Printing Office, 2013.
[13] D. Yost and R. Nieto-Gomez, "NATO's preparedness for cyberwar," Monterey, California: Naval Postgraduate School, 2016.
[14] S. R. Kumar, S. A. Yadav, S. Sharma, and A. Singh, "Recommendations for effective cyber security execution," in *Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference on*, 2016, pp. 342-346.
[15] N. A. M. Z. Mahfizah Mazlan, Jamaludin Ibrahim, "A Cyber Security Assessment of Muslim Countries," *International Journal of Information and Communication Technology Research*, vol. 6 No, p. 8, 12, December 2016 2016.
[16] K. N. Sevis and E. Seker, "Cyber warfare: terms, issues, laws and controversies," in *Cyber Security And Protection Of Digital Services (Cyber Security), 2016 International Conference On*, 2016, pp. 1-9.
[17] A. Kott, C. Wang, and R. F. Erbacher, *Cyber defense and situational awareness* vol. 62: Springer, 2015.
[18] T. Jianqun, " Cyber War Preparedness, Cyberspace Arms Control and the United States," China Institute of

International Studies (CIIS) 3, Beijing, August 2014 2014.
[19] P. W. Singer and A. Friedman, *Cybersecurity: What everyone needs to know*: Oxford University Press, 2014.
[20] M. G. Z'hra, "NATO'S PREPAREDNESS FOR CYBERWAR," 2016.
[21] Eurotherm, *Cybersecurity Good Practices Guide*, 2017.
[22] M. J. Haber and B. Hibbert, "Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations," 2017.
[23] R. Slayton, "What is the cyber offense-defense balance? Conceptions, causes, and assessment," *International Security*, vol. 41, pp. 72-109, 2017.