Law and Political Science Journal

Volume:08/ N°: 02 (2022), p 710-718

Received 07/04/2022 Accepted27/08/2022

Strategic mechanism of combating cyber crime under the new environment of digital communication

Nabil Chaib

Military Higher School Of Information and Communication (Algeria)

chaib.nabil@univ-medea.dz

Abstract

This research paper discusses the problem of cyber security in light of digital changes, by presenting the concept of cyber security and its terminology and concepts, especially with the growth of cyber threats, so the idea of deterrence in the new communication environment has become part of these security strategies for countries.

Through this article, we aim to highlight the functional purposes of the issue of cyber informatics security, which has become a major regional and global challenge, particularly with the increasing cyber security threats, and Algeria, like other countries, has since sought to protect its information system through many security devices and cells.

Based on the results of the explanation, we have reached through this study the need to adopt and modify the standards and practices adopted in the digital environment, and follow up the development of procedures to deal with all issues related to safety and cyber security, especially that cyber threats represent a real threat to cyber security because of the difficulty of identifying and tracking the perpetrators of cyber attacks.

Keywords: Cyber crime, cyber attack, network security, digitization, security strategy

ملخص:

تناقش هذه الورقة البحثية إشكالية الأمن السيبراني في ظل التغيرات الرقمية ، من خلال عرض مفهوم الأمن السيبراني و المصطلحات و المفاهيم الخاصة به خاصة مع تنامي التهديدات السيبرانية ، لذا باتت فكرة الردع في البيئة الاتصالية الجديدة جزءا من هذه الاستراتيجيات الأمنية للدول .

نهدف من خلال هذا المقال إلى إبراز المقاصد الوظيفية لقضية الأمن المعلوماتي السيبراني الذي أصبح من التحديات الكبرى على الصعيدين الوطني والعالمي، لاسيما مع تزايد التهديدات الأمنية الإلكترونية، والجزائر كغيرها من الدول سعت منذ انتهاجها للإدارة الإلكترونية حماية منظومتها المعلوماتية من خلال العديد من الأجهزة والخلايا الأمنية.

واستنادا لنتائج التحليل، توصلنا من خلال هذه الدراسة إلى ضرورة اعتماد وتعديل المعايير والممارسات المعتمدة في البيئة الرقمية، ومتابعة تطوير إجراءات التعامل مع كافة المسائل الخاصة بالسلامة والأمن السيبراني، خاصة و أن التهديدات السيبرانية تمثل خطرا حقيقيا على أمن الفضاء الالكتروني لصعوبة تحديد و تتبع مرتكبي الهجمات السيبرانية.

الكلمات المفتاحية : الجريمة الالكترونية ، الهجمات السيبرانية، الأمن السيبراني ، الرقمنة ، الاستراتيجيات الأمنية

.

1. *Introduction*

This study is part of a study aimed at establishing a National Cyber security culture, especially since the starting point of National Cyber security is the formulation of a national policy to raise awareness of cyber security issues and requires national action and cooperation International.[1]

The second step is to formulate a national cyber security stimulus plan to reduce the risk and impact of cyber threats, and participate in international and regional efforts to promote national prevention and cyber accident recovery.

With the development of the information and electronic revolution and the wide spread of the network, its closed door was opened, its events were covered up, and it issued an alarm without guards, [2] Restrictions or restrictions to prevent bad things caused by human beings in the past and now.

Due to the proliferation of scientific and technological discoveries, so-called cyber crimes or cyber attacks have emerged. These crimes or cyber attacks have brought great danger to society, and their professionals have committed acts of robbery, destruction and threat to the security of many countries.

1. *Research Methodology*

2.1 Main research questions

Therefore, these countries have taken a strict position to reduce this serious phenomenon and need to understand what cybercrime is, what the purpose of its dissemination is and how to prevent it.

Therefore, we must ask the following questions:

What cyber security mechanisms can be used to tackle cybercrime?

2.2 Research questions

- What are the levels of cyber security for confronting cyber threats?

-How does infrastructure contribute to activating cyber security to confront cybercrime?
-What are the ways and mechanisms to avoid cyber attacks in the new communication environment?

2.3 Research objective

The purpose of this study is to explore political, communication and asymmetric security threats, explore the characteristics and functions of different media, measure the impact of media activities, and evaluate the effectiveness of communication efforts.

In addition to all data and information on communication activities, models and models, media practices, media systems and other factors emphasize the need and growing need for information and communication research, especially An infectious political party and psychological warfare practitioner crossed the virtual space.

2.4 Defining concepts and terminology

Cyberspace: It is the space created by information and communication technology, primarily the Internet. This space is closely linked to the physical world, through various communications infrastructures, information systems and through many services, without which, no less, access to data and information could not be obtained. [3]**Infrastructure**: Devices and equipment, used to connect computers, are between the latter and their users. Infrastructure includes media, including telephone lines, cable TV lines, satellites and antennas, as well as routers, assembly, and other devices that control transmission paths.

It also includes programmes that are used to generate associated services, related to that (technology) that accompanies them, general software, associated development and maintenance services, and networking lines that link that software.[4]

Cloud computing: Access to a common communications and information services infrastructure, such as networks, services, applications, and data stores, which can be provided and secured, with minimal service provider intervention.[5]

Cybercrime: Cybercrime considers such unlawful conduct relating to the automated processing and transmission of data to be either a means used in the commission of the act or the environment and the medium in which the offence occurs, and the purpose or purpose of the offence to commit the criminal act.[6]

2. Cyber Security: Causes and Repercussions

The transformation from society to information society is realized by integrating new technologies into every field of activity and every infrastructure, thus increasing the dependence of individuals, organizations and countries on the system.

Developing countries, including Algeria, faced the need to join the information society, bearing in mind the risks and needs of their shift to reliance on technology and technology providers in order to avoid the risk of a digital divide. It creates security vulnerabilities and even over reliance on institutions that control their needs and implement information technology security means.

Interconnected information technology system is a resource that can be accessed remotely, so it may become the target of network attack. The risk of invasion is also high because of the increasing possibility of attack and crime.

Although these regimes are the targets of attacks, the spoils sought by the attackers are the information being processed.

Such attacks may undermine the ability to process, store and share information assets and may even undermine the organization's intangible and symbolic goods, production and decision-making processes. Pass on the risk of owning these operating systems to the organization.

Therefore, it may be relatively difficult to deal with complex and multifaceted cyber security issues, and its potential complexity and its impact on organizational and national operations may be devastating. Key factors for economic success may depend on the ability to provide security for information, operations, systems and infrastructure.

3. Classification and types of cyber crime

Cybercrime is divided into:

* Crimes against elements (confidentiality, integrity, richness of data and systems)
-Illegal (unauthorized) entry: a person invades the network and computer connected to the Internet, invades the network security system, enters the machine and divulges its contents. Illegal opposition.
-Data destruction (this command is issued after the network is invaded by hackers, the data is scanned, the data is destroyed, and the stored program is disabled, making it unusable).
***** Computer related crimes include**:**
-Computer related forgery.
-Computer fraud.[7]
* Content related offences include one category of offences under this Convention, namely those related to pornography and immoral acts.
* Crimes related to copyright infringement and software piracy.
-Cybercrime by data type and crime location:
-Crimes affecting computer data sharing.
-Offences affecting personal data or personal means of life.
-Crime of infringing intellectual property rights of computer software and systems (Crime
f software piracy).[8]

4. **Preventive mechanisms against cybercrime**:

5. In order to reduce cybercrime, almost all countries and individuals must contribute as much as possible to combat it by:

6. 1. Reasoning, including inspection, inspection and expertise, involves the particularity of cybercrime.

7. 2. International and domestic efforts to legalize the prevention of this new crime, and the efforts of international institutions and organizations are:

8. • Raise public awareness of cybercrime and recognize that cybercrime is a threat that must be faced and ensure that they do not become victims.

9. • Electronic addresses that require confidential information, such as credit cards or bank accounts, need to be identified.

10. • Don't disclose passwords to anyone, make sure to update them regularly, and choose unfamiliar passwords.

11. • Do not save personal photos on your computer.

12. • Do not download any files or programs from unknown sources.

13. • Pay attention to updating the protection system, such as using Norton and other protection software wait

14. • Set up an organization to fight against cybercrime.

15. • Track the development of cybercrime and formulate information, devices and legislation to combat cybercrime.

16. • Develop secure software and powerful operating system to limit electronic intrusion, virus and spyware, such as anti spyware, that is, scan the computer to search and delete Spyware components, such as Lavasoft.[9]

17. International efforts to combat cybercrime through the digital communication environment

The former legal system depends on a crime committed in a geographically identifiable place, but information crime is a crime committed in an undeterminable theater, but it includes the largest human grouping characterized by complex association and entanglement, the most important characteristic of which is the creation of special mechanisms to impose obligations and comply with them such as disconnecting hackers from certain rules or expelling them from forums, but this huge human gathering lacks common moral standards.

This is why the European Council concluded the aforementioned Podest COUNCIL Agreement, which provided images to combat these crimes, article 22 of which stipulates that each party shall take legislative and other measures that it deems necessary to determine its jurisdiction for each crime that occurs in accordance with articles02- to 11 of the current Convention when the crime occurs:

- Within the local scope of the state
- On board a ship carrying the flag of that country.
- On board a plane registered in this country.
- By one of its nationals, if the crime is criminally punishable at the place where it was committed or If the crime does not fall within any jurisdiction of any other country.[10]

The Council of Europe Convention on Cybercrime, to which the U.S. is a signatory, defines cybercrime as a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements.

The necessity of internet connectivity has enabled an increase in the volume and pace of cybercrime activities because the criminal no longer needs to be physically present when committing a crime. The internet's speed, convenience, anonymity and lack of borders make computer-based variations of financial crimes - such as ransom ware, fraud and money laundering, as well as crimes such as stalking and bullying -- easier to carry out.

Cybercriminal activity may be carried out by individuals or groups with relatively little technical skill, Or by highly organized global criminal groups that may include skilled developers and others with relevant expertise. To further reduce the chances of detection and prosecution, cybercriminals often choose to operate in countries with weak or nonexistent cybercrime laws.

Cybercrime attacks can begin wherever there is digital data, opportunity and motive. Cybercriminals include everyone from the lone user engaged in cyberbullying to state-sponsored actors, like China's intelligence services.

Cybercrimes generally do not occur in a vacuum; they are, in many ways, distributed in nature.

That is, cybercriminals typically rely on other actors to complete the crime. This is whether it's the creator of malware using the dark web to sell code, the distributor of illegal pharmaceuticals using crypto currency brokers to hold virtual money in escrow or state threat actors relying on technology subcontractors to steal intellectual property (IP).

Cybercriminals use various attack vectors to carry out their cyber attacks and are constantly seeking new methods and techniques for achieving their goals, while avoiding detection and arrest.[11]

18. **Strategic security mechanism for combating Cybercrime**

19. The purpose of network security is to help protect an organization's organizational, human, financial, technical and information assets and resources so that it can perform its tasks.

The ultimate goal is to ensure that the organization is not permanently damaged. This will include reducing the possibility of reflecting risks, reducing the resulting damage or poor performance, and ensuring that normal operations return to normal within an acceptable time and reasonable cost after a security incident.

The process of network security involves the whole society, and everyone is interested in implementing it. This process can be made more important through the development of cyber codes of conduct and the publication of real security policies that set standards to be met by users, entities, partners and suppliers.

Security solutions exist, but they are by no means absolute. Generally speaking, they only represent the response to specific problems in specific situations. As a result, the safety problem is shelved, the safety responsibility is transferred, and the solution also needs insurance and protective management.[12]

Security strategies are often limited to the establishment of security mechanisms to reduce the risk to the company's information assets, usually taking a purely technical approach. A better strategy is one that takes into account all aspects of the problem and meets individual security needs, especially with regard to confidentiality and fundamental rights.

The overall consistency of the security strategy is complex because it involves a wide range of different entities and individuals (engineers, project developers, auditors, system engineers, investigators, customers, suppliers, etc.). Due to a wide range of interests, vision, environment and language.

A unified and systematic understanding of risks and safety measures is needed. Every responsibility involved must be recognized if the level of security required for clandestine activities using information and communication technology is to be achieved and contribute to confidence building, Digital economy.[13]

In a sense, it is a tool of psychological warfare, that is, in order to achieve its goal, it is all means of communication from personal contact to mass communication, from news, drama, radio, television and the Internet[14].

The objectives can be summarized as follows:

-Question ability and self-confidence, spread negative emotions, create despair, shake beliefs, shake trends, and undermine authority.

-Prepare the public for acceptance and reception.

Undermine faith in principles and goals.

-Shoot unreal things, zoom in, twist and color.

-Weaken the hostile domestic front, reduce its morale, create loopholes within it, and confuse decision-makers and decision-makers.

-By creating crises, taking advantage of differences, taking advantage of contradictions among the people and questioning the integrity of the target state institutions, we can split the country, unify and split the country, and encourage some parties to sacrifice others.

-Explain its achievements and activities in various areas and support them.

-Release the energy of the target person, and change his power, calculation and balance by influencing his thought, emotion, direction, belief, theory, mental state and will, so as to consume the fuel and power of his work.

-Damage social ideology, national philosophy, national personality and national image in international relations.[15]

John Scott, an American writer and journalist, said in his guide to the coexistence of political war and competition that the main purpose of political and psychological war is to weaken the enemy and, if possible, destroy and isolate the enemy through tactics, pressure and manipulation of information. Make the news colorful.

Therefore, psychological warfare, [16]as the stage of its action and the field of its action, is the root, hope, instinct and emotion of human psychology.

Its purpose is to weaken human psychology, give play to its strings and go deep into its heart.

In short, strategic war is directed against all the people and all their components, capabilities and categories, while tactical war is only directed against the armed forces, which are carried out in the actions to achieve the objectives of the war.[17]

A series of factors related to and affecting cyber war make this role more important. These factors highlight the increasing need to use research, the most important of which is the need to collect accurate data and information on the problem. Environmental, social, cultural and economic impacts and the extent to which information contributes to addressing these issues, and there continues to be a need for sustained data and information on public opinion, trends, beliefs, opinions and views In view of the importance of studying public opinion and its influence in media activities, as well as studying audiences, readers and listeners The audience should fully understand their situation and help to provide them with appropriate information materials.[18]

20. **Research results and suggestions**

Through the critical interpretation of the theory of network security and how to deal with network crime, we draw the following conclusions and suggestions:

- Establish network security awareness, educate and train all stakeholders of network security
- Develop a National Cyber security strategy and protect sensitive information infrastructure

• Establish national computer accident management capability to curb cyber crime
• Supervise the establishment of a Maghreb and Arab network as a framework for cooperation between them and coordinate with similar international centers and other security agencies engaged in related or complementary activities.
• Recommend and establish an appropriate framework for judicial and security institutions to exchange information and experience in combating cybercrime and protecting the safety and security of cyberspace
• Adopt, revise and further develop procedures to address all cyber security and security issues
• Develop model laws to regulate issues related to confidence building in cyberspace, information and knowledge society, such as e-commerce, data security, information system security, personal data protection and non content management Projects and harmful content, electronic signatures, signature authentication services, criminal investigations and prosecutions, tracking, monitoring and evidence, e-government applications, privacy protection and freedom of information in the communications sector E-commerce, intellectual and industrial property rights, neighboring rights, electronic transaction security, online child protection, etc...

21. *CONCLUSION*

Cyberspace and its related technologies and information tools are an important aspect of future conflicts and conflicts, involving various fields. Especially with the development of science, the tools and means of cybercrime have been greatly developed. It involves all social, economic and political fields, so fundamental solutions must be developed to solve the phenomenon caused by this development and reduce its spread in society.

Therefore, countries strive to maintain their important electronic technology structures and defense systems, especially in the face of the modern digital revolution, and a virtual space has been generated on the basis of the global information and communication technology structure Cyber attack is an important legal issue in contemporary international law.

***Bibliography List* :**

[1] Amir Faraj Yusuf, cybercrime, University Press, tower 1, Egypt, 2001,p75

[2] Bulueliv. cyber threat intelligence for Banking &Financial services. spain: Bulueliv. 2019 ,p52

[3] Munira bent Fahad Hamdan, "cybercrime when technology becomes a means of crime", Al Jazira, Jordan, 2007,p77

[4] Abdessabour Abdel qawi, cybercrime and international efforts. Egyptian publishing and Distribution Company, tower 1, Egypt. 2011,p124

[5] Opcit,p144

[6] Rahmah El dalmakhni, types of cybercrime, summary house, Bahrain, 2017 ,p19

[7] Tolido, R. , Reinventing Cyber security with Artificial Intelligence: The frontier in digital security. Capgemini Research Institute, Paris,2019 ,p76

[8] Tolido, R. Opcit, p77

[9] Joseph S. Nye, Deterrence and Dissuasion in Cyberspace' , International Security , Volume 41, 2016.

[10] Guercio, K, Top 22 Cyber security Startups to Watch in 2021. Retrieved 14/02/2022, from Security Planet: www.esecurityplanet.com

[11] Kate brusch , cyber crime , https://www.techtarget.com/searchsecurity/definition/cybercrime , 17/02/2022 , 14 h

[12] Bouveret, A, cyber security for the financial sector: A Framework for Quantitive Assessment. Working paper, IMF.2018,p63

[13] Bouveret, A , Opcit ,p75

[14] Ibid,p102

[15] Guercio, K, Top 22 Cyber security Startups to Watch in 2021. Retrieved 14/02/2022, from Security Planet: www.esecurityplanet.com

[16] UN General Assembly. General Assembly Resolutions. New York: United Nations, 2020, www.un.org/en/sections/documents/general-assembly-resolutions/

[17] Carnegie endowment for international peace. , Timeline of cyber incidents Involving Financial institutions. Retrieved 02 /17/ 2021, from Carnegie endowment for international peace: http:// carnegieendowment.org

[18] cyber Intelligence House. Cyber Expo-sure Index. Retrieved 15/02/2022 from cyber Intelligence House: http://cyberexposureindex.com