The Effect Of Cyber Threats On Homeland Security, Cyber War As An Example

Dr. Ahmed Kerbouche[1], Dr. Lakhdar Miloudi[2]

[1] Laboratory of Legal and Economic Studies, Aflou University Center, (Algeria)
Email : a.kerbouch@cu-aflou.edu.dz
[2] Laboratory of Legal and Economic Studies, Aflou University Center, (Algeria)
Email : l.miloudi@cu-aflou.edu.dz

Received: 16/09/2024; Accepted: 11/12/2024; Published: 15/01/2025

Abstract:
Battlefields have witnessed the appearance of a new generation of fighting methods, which relied on electronic technics and computers in managing different battles known as cyberwar. This war is considered among the threats on homeland security of countries. Its results are very big, due to its negative effects on different fields. That is for the sake of control and eliminate the country's inferstructure. The aim of this study id to identify this cyberwar and its types, also we tackle some forms of cyber defense and protection.

Keywords: Cyber threats, Cyberspace, Cyberwar, National security.

Introduction

Research Problematic:

According to what has been dealt with, the study problematic lies on this question:

At what extent cyberwar effects homeland security, and what is the countries' power to control and dominate this field?.

A number of questions branches from this study and they are as follows:
What is intended by cyberwar?
What are kinds of cyberwar?
What are cyber security and defense methods?

Followed course:

This study is classified among the descriptive researches where we deal with the research problematic by appointing the meaning of cyberwar and relying on different printed and digital resources.

Also it was focused of the course studying the state in order to identify the study's unit of cyberwar as an example from other cyber threats, and that is in a detailed and specific manner that allows as to gather information and data which would help us to arrive at clear results.

Introduction: By the end of the previous century, a boom has happened in technological progress. And that is information technology from automatic accounts and network connections, which led to the appearance of the word: Cyberspace.

Cyberspace is a development that worked on getting millions of people and communities closer. It has given new opportunities to gain information and exchange it in no time, no more than seconds.

From another side, Cyberspace contains great threats, including cybercrimes.

Which are divided into the following types: cyber terrorism, tapping, cyberwar, hacking, spying and others. It is considered among the most important threats on communities, individuals, and nations. It has left the feeling of insecurity and distrust. Other kinds of threat has appeared, such as: drug crimes, money laundering. Cyberwar is one of the key subjects in global conflict. It confirms the location of countries based on who has the most defense and attack on the other. The latter has affected all economic, political and cultural life aspects. Who owns the power of technology of information, owns the scale of power in the world. Whereas, we have moved from taking over earth and nation sovereignty to taking control over cyberspace.

Some terrorist organization has already websites and owns high tech materials that is able to hack any country to recruit thousands of people to include in its agenda. That is why it had become necessary for all countries to work together to protect cyberspace. That is through many mechanisms.

Problematic:

- To what extent cyberwar affects homeland security, and what is the ability of nations to control this field?

First Chapter: The theoretical frame of the study.

We tackle the definition of some concepts represented in cyber threats and cyberspace, and then we identify homeland security as follows:

1- The definition of cyber threats:

Threat in language is from the verb threaten, it results in hurting and damaging. Threat is related to anything that disrupts the process of building security and leads to feeling less secure.

It is meant by cyber threats, those attacks that are done using mechanisms and electronic networks such as Internet and computers. It aims to damage electronic devices or electronic networks, or stealing information from it.

Identity theft, dangerous malware, tapping, fraud, spying and hacking are among cyber threats.

2- The definition of Cyberspace:

Cyberspace is a group of computer networks around the world, and everything connected to it and controls it. It is not limited to the internet web only, it includes a lot of computer networks. Cyberspace includes all computer networks that runs the activity of countries and its institutions and departments and everything related to its vital environment. In all civil and military sectors. [2]

The international union of communication defines cyberspace as the physical space and else, it consists in many elements, which are: computer devices, networks, software, computer information and the users of the mentioned elements.

Cyberspace works under physical and untraditional circumstances where it is an intermediary through working from computer devices and connection networks. One goes to these virtual spaces because they are digital and geographically unlimited.

---

[1]Yleasal Bent Nabi Yasmine, Amrouch Elhousain, cyber-threats and cyber-security in Arab world, magazine numiros academy, book 2, number 2, 2021, p164

[2]Salah Hyder AbdElwahid, cyberspace wars, a study in its meaning and components, and ways of confronting it, masters dissertation, department of political sciences, faculty of letters and sciences, university of Middle East, 2021, p17

[3]Fatima Biram, national sovereignty in the light of cyberspace and digital changes, China as an example, magazine Algerian for human security, 5th year, number 5, January 2020, p793

It allows to every person who ever they are and wherever they are to express his thoughts without fear or hesitations.

Through building interaction with no time and space borders. It provides him with the possibility of carrying on

with his life in this space that is known with lying information at a speed of light and distance cancelling.

Cyberspace has a role in inferstructure transaction in international relations. It started moving its influence of inferstructure to making changes on the world system. The world has witnessed a development in security risks, with the development of technological maturity stages. The issue of cyberspace has become an international security issue, especially after the events of 09.11 , where it is looked at as a new security threat. [2]

3- The definition of homeland security:

It is known as a group of economical, diplomatic and political aspects, in addition to the military aspect. Arnold Walvers has given such definition when he said: '' Security is measured by its subjective meaning, as far as the absence of guided threats to the acquired values. And it appoints with its self-meaning to the absence of fear rather than those values facing an attack'' [3]

Henri Kesinger defines it as '' Any behaviors that a society by witch it seeks its survival right '' [4]

The relationship between Cyberspace and Homeland Security where the content lies with its whole meaning in military, intellectually, politically, economically and informatically meaning. Especially with the spread in adopting electronic government by side many countries. And the spread of the users of means of communication and information in the world. Where homeland databases become vulnerable to outside, and being contentiously exposed to cyber threats.

Chapter two: cyberwar and its repercussion on the countries and their homeland security.

We tackle in the chapter the definition of Cyberwar and its kinds, and arrive at some cyber-confrontation between nations as follows:

[1] Philippe engelle hard, l'nternet change – t – il vraiment nos societés toms edl harmattan paris, France, 2012, p 38

[2]Nacira Salhi, Intelligent Power, global competition on cyberspace power and cyber-abilities, book of politics and law, book 13, number 01, 2021, p 379

3 Arnold Wolfers, Discord and collaboration, Essays on International Politics (Baltimore: John Hopkins University Press, 1962), P.150.

4 Henry Kissinger, Nuclear Weapons and Foreign Policy (London: Wild Field and Nicholson, 1969), p 46.

5Adel Abdsadik, cyberspace weapons in the light of the international human law, series of papers, number 23, Unit of future studies, Alexandria, Egypt, 2016, p16, p17

1- The definition of Cyberwar:

Abdelkader Muhamed Fahmi as: attacks use web system, and computer devices for the state, or users besides countries. To dismantle the ability to control in a system of devices or computer networks with data and information of users from other countries. Meaning to control or eliminate on the level of the national inferstructure of a country, in a form that exposes homeland security to a real threat.

Richard Klark defines cyberwar as: an authorized hacking a network or computer of a country by another government or a support to it or ant activity that effects a computer system in the intention of changing or faking data. Causing a computer device dysfunction connected to a network, or the things that a computer system controls. It is described as actions a state takes to attack information systems of the enemy, to effect it and defend its information systems.[2]

Although the specific features of any cyberwar are still not marked. However the big attacks on information inferstructure and Internet services in the last decade gives a picture on the possible shape and field of conflict in Cyberspace.

2- Types of cyberwars and its effects on homeland security:

Kinds of cyberwar vary from electronic disturbance, website hacking and electronic spying. It is as follows:

A- Disturbance operations or electronic attack:

These operations use electromagnetic power to locate the opposite target websites and directing weapons to hit it with high accuracy. With the attempt to effect electronically the enemy's electronic systems to dismantle it.

-

[1]Salah Haider AbdElwahid, cyberwars, a study in its components and ways of confronting them, previous source, p 08

2 Schmitt, M.N,(computer network attack and the use force in international law through on normative), the Colombia journal of transitional law, Vol.27,No. 885,1999, p. 07.

In other words, it is a group of decisions taken to prevent the affective use of the spectrum or dismantle the enemy's systems and electronic means.

B- Website Hacking:

Hacking in general in the arrival at a certain goal illegally, through holes in the security system of the targeted computer, to achieve many goals that disturbs the security and sovereignty of the country. Through changing the content s of the targeted website by the attackers, stealing sensitive information, shutting the website down, or taking control of it generally using what is known as the software of the counting virus. It became a real threat, with a significantly dangerous effect in the last few years, on operation systems or computer networks. Looking at the large capacity of exchanging files and software between network users, and computer viruses. It is a software cloning itself in the affected device when they are active to make changes in programs or the nature those programs work in. Which causes various damages and they vary between spam messages pooping for the user or the loss of stored files, and it may also cause crashing the operating system.

In some cases the hacker (intruder) uses the already affected device as a tool to launch an attack on another device, especially if they are connected to the same network. This king of attacks requires gathering information on the system or the network that is being hacked. Recognizing its security and operating systems, by taking advantage of its weaknesses to hack it easily.

One of the most apparent examples of these attacks is what the American Ministry of Defense has announced in 1196 that there are about 250,000 hacking attempt on the operating system of the ministry. 75% of these attacks have indeed succeeded. The pentagon declared that they are about 150 hackers have been caught planning to attack the operating system of The American Aviation Forces.

C- Web spying:

It is the use of modern information technology to gain unauthorized and illegal access to web-information systems of countries and government and tapping them to gain its information. Information related to its system and secrets, and it includes all the military, security, political, economical, cultural and social information.

[1]Dr, Adnan Enakib, cyberwar in the light of protocol seventy-seven in The four Geneva conventions of the year 49 (cyber-attacks) Arabic Center, Egypt, 2022,p 101, p 105.

Spying movements has been active since the attacks of 09-11-2001 in the USA, when The US security agencies revealed its spying on the Internet and started wide operations to hunt what they call ‘’terrorist groups’’. Many questions have been

raised about using those anti-USA groups the Internet to command the sleeper cells.

In general, Cyberwar could be divided into three main levels:

-Level one: It is the operations accompanying traditional wars to achieve knowledgeable upper hand, like attacking the aviation defense system. Which leads to wide strategic losses due to the importance of aviation defense to countries.

-Level two: They are limited cyberwars that the inferstructure and civilian targets are attacked. [1]

-**Level three:** Unlimited cyberwar that the attackers aims to enlarge the destructive effects to the inferstructure. Where it reflects negatively on the social engineering of the country, like attacking capital markets, emergency services, electronic systems of power generators and other goals that follows wide destructive effects. The aim of this kind of wars is to expand the range of losses as much possible.[2]

Generally speaking, the effects of cyberwar on homeland security of countries are:

-The increase of cyber dangers: Especially with ability of the vital, civil and military facilities to be attacked. The thing that effects the functions of these facilities, as a result controlling the execution of the attack is considered a strategic tool of control.

-Reinforcing and spreading power: Cyberspace worked on reconstructing the ability of participating parties and lead to the spread of power between multiple users.

-**Militarizing cyberspace:** Many parties appeared in this frame, such as development in the field of defense policies and cyber security, and the increase of capabilities in cyber armament race. Adopting defensive policies

[1]Noran Chafik, the effect of cyber-threats on international relations, a study in cyber-security, Arabic Office of Knowledge, Cairo, 2016, p39

[2]Noran Chafik, the effect of cyber-threats on international relations, a study in cyber-security, same previous source, same page.

in defense and security facilities. As well as the increase of investment in the field of developing cyberwar tools inside

modern armies.

-Integrating cyberspace into the homeland security of countries:[1] That is through updating armies and forming special forces in cyberwars and establishing national organizations to defend cyber security.

The increase of cyber dangers lead to changing the content of homeland security and countries became looking to redefine its homeland security. With the appearance of a new cyberspace front, as a threat to the security of countries. Which led countries to insert it with its homeland security strategies, and the search to develop its abilities in the field of defense, protection and attacking, and updating its armies to deal with the new cyberwar. Cyberspace has become a field of increasing threats, and in this table shows cyber-attacks that some countries have launched against other countries.

It is a study done by Brandon Valriano and Rayan Manis by gathering specific date on electronic confrontations around the world between 2001 and 2011 and they are as follows:

Table (1) shows electronic confrontations between countries

Number of attacks done by country A	Number of attacks done by country B	Number of attacks done by both parties
China (20)	USA (2)	22
Pakistan (7)	India (6)	13
North Korea (10)	South Korea (1)	11
Israel (7)	Iran (4)	11
China (7)	Japan (0)	7
South Korea (4)	Japan (3)	7
USA (6)	Iran (1)	7
China (5)	Taiwan (0)	5
China (4)	India (0)	4
Russia (3)	Georgia (1)	4

Russia (4)	Estonia (0)	4
Russia (3)	USA (0)	3
North Korea (3)	USA (0)	3
China (2)	Vietnam (0)	2
Lebanon (1)	Israel (1)	2
North Korea (1)	Japan (0)	1
India (1)	Bangladesh (0)	1
Syria (1)	USA (0)	1
Kuwait (1)	Iraq (0)	1
China (1)	The Philippines (0)	1

-valeriano and ryan c maness; the dynamics ofcyber conflict between rival antagonists, 2001 – 11 journ al of peace recearch, vol 51no 3, april, 2014, pp 356 .

[1]Dr, Lamia Tala, Threats and cyber-crimes and its effect on homeland security on countries and the defense strategies, magazine of Maalim for law and political studies, book 04, number 02, 2020, p 59.

The table shows that China and USA are in the lead, as they both witness multiple cyber-attacks, most of them from China. 20 attacks According to data that the study shows. Pakistan and India come second with 13 cyber-attack.

As also shown that Iran was involved in the conflicts against the USA from a side, and against Israel from another side. It received 6 cyber-attacks from USA and 7 from Israel.

Russia has launched at that period, 3 of them against Georgia, 3 against USA and 4 against Estonia according to the study.

Chapter Three: Examples of cyber defense and protection for countries

Methods and mechanisms of cyber-defense are many. By which a country could protect its cyber systems from outside

attacks, that they became to some a new world reality. It is very complex, we arrived at traditional war words added the virtual and cyber adjective to it, such as cyber-race, cyber battle fields, cyber-Jihad. Some of the world power countries nominated in the field of cyberwar for what they have are USA, China and Russia.

1- The united States of America:

When we take a closer look at The USA's policy, we find that it does not hold just defensive meaning in its negative prospective. Preventing enemies from gaining access to its computer networks and blocking cyber-attacks, whereas its biggest part is on the understanding of active defense. Which means searching for enemies and pointing threat sources and attacking them before it became an active state. It means that in other words that defense goes beyond the measures of entry surveillance, intruder detector and firewalls.

It includes protective strikes before threats turn into the high dense active state. Especially when it comes to terrorist cyber-attacks and organized crime.

Even the cyber-rebellion especially for the defense planners. The principle of active defense the search and attack threat resources before they appear.

That means in other words, it surpasses the traditional meaning that focuses on reinforcing counter defense breaches. Spying, viruses, piracy and other, yet it requires doing protective strikes such as shutting down counter network websites. Hacking suspected cyber-accounts, call tracking, dismantling encrypted messages and other. These activities appear attacking, yet they are for defensive porpuse, which was takes from the idea of Clausefitz about attacking for defense.

2- People's Republic of China:

China put a lot of interest on cyberwar during the last decade; it expanded its cyber-capabilities. It took the document of ''the complete cyber-web for war'' as a main document. China's interest moved to combine all cyber and non-cyber sides of war of information inside one authority. Since 2008 all the main operations of the army include Internet components and the informational operation that had a defensive and attacking nature at the same time.

The army was reorganized in 2015 through creating three new organizational branches including the power of the first strategic support to deal with intelligence and military operations in cyberspace. The second for military operations in space and satellites and the third is responsible of the attacking and defensive abilities and artificial intelligence.

3- Russia:

Russia has announced in 2010 its military ideology, which points out that modern military conflicts require the complete use of military force with the interest more in the war of information. An independent authority for cyber security was formed to defend against cyber-attacks and taking the protective decision against

---

[1]Amir Mesbah, cyberspace, example for expanding cyber-defense ideology. Magazine of defense studies and supervision, number 16, p90, 2021

[2]Dr, Dalila Eloufi, cyberwar in the age of AI, and its bets on internation security, magazine of wisdom for philosophical studies, book 09, number 02, 2021, page 795.

cyber-attacks through networks. Russia bought typing machines to use in vital libraries so not to be hacked. The volume of Russian military expense on cyber-war 127 million dollars from a total military expense of 40 billion dollars. Russia is forth in the world in the field of developing cyber-weapons.[1]

Conclusion:

Cyber-war is considered among the key points of conflict in cyberspace battlefields, especially with the development of different technology means and the appearance of many users suck as non-governmental organizations and radical movements. They could threaten the sovereignty of any country with simple tools. That is why military force is not the only threat for countries, but owning cyber-power has a great risk on targeted countries.

Homeland security is no longer limited on military security only. We are in front of the reality of homeland cyber-security. Who owns the information is the one who has power.

Finally, we indicate some important recommendations and they are as follows:

1- Forming national fronts specialized in cyber-security, because cyberwars do not separate between military and civil aspects. These fronts' missions is to raise the level of cyber-awareness and preparing the national strategy of cyber-security and different instructions with it.
2- Building cyber-armies and having budgets to develop the field of protection, attack and defense. In this frame, The US is the lead in building cyber-armies and having huge budgets for it, where is spends about 7 billion dollars annually of cyber-security.

3- It is important to activate the tech mechanism, in its from come protection walls or firewalls that are considered the most import tech to block cyber-attacks. It separates trusted and not trusted zones including computer networks. Also it monitors all the operations that goes through the electronic web.

[1]Amani Aissam, Russia and the use of cyber-power in managing its international relations, p173, on the link:

https://jpsa.journals.ekb.eg/article_200069_efa19d1f2a8f15faf259e9d8822f7d8b.pdf

Bibliography List setting :

-Yleasal Bent Nabi Yasmine, Amrouch Elhousain, cyber-threats and cyber-security in Arab world, magazine numiros academy, book 2, number 2, 2021, p164

1. Salah Hyder AbdElwahid, cyberspace wars, a study in its meaning and components, and ways of confronting it, masters dissertation, department of political sciences, faculty of letters and sciences, university of Middle East, 2021.
2. Yleasal Bent Nabi Yasmine, Amrouch Elhousain, cyber-threats and cyber-security in Arab world, magazine numiros academy, book 2, number 2, 2021, p164
3. Fatima Biram, national sovereignty in the light of cyberspace and digital changes, China as an example, magazine Algerian for human security, 5th year, number 5, January 2020, p793.
4. Philippe engelle hard, l'nternet change – t – il vraiment nos societés toms edl harmattan paris, France, 2012.
5. Nacira Salhi, Intelligent Power, global competition on cyberspace power and cyber-abilities, book of politics and law, book 13, number 01, 2021, p 379
6. Arnold Wolfers, Discord and collaboration, Essays on International Politics (Baltimore: John Hopkins University Press, 1962), P.150.
7. Henry Kissinger, Nuclear Weapons and Foreign Policy (London: Wild Field and Nicholson, 1969), p 46.
8. 5Adel Abdsadik, cyberspace weapons in the light of the international human law, series of papers, number 23, Unit of future studies, Alexandria, Egypt, 2016, p16, p17.
9. Salah Haider AbdElwahid, cyberwars, a study in its components and ways of confronting them, previous source, p 08
10. Schmitt, M.N,(computer network attack and the use force in international law through on normative), the Colombia journal of transitional law, Vol.27,No. 885,1999, p. 07.
11. Dr, Adnan Enakib, cyberwar in the light of protocol seventy-seven in The four Geneva conventions of the year 49 (cyber-attacks) Arabic Center, Egypt, 2022,p 101, p 105.
12. Dr, Lamia Tala, Threats and cyber-crimes and its effect on homeland security on countries and the defense strategies, magazine of Maalim for law and political studies, book 04, number 02, 2020, p 59.

13. Amir Mesbah, cyberspace, example for expanding cyber-defense ideology. Magazine of defense studies and supervision, number 16, p90, 2021
14. Dr, Dalila Eloufi, cyberwar in the age of AI, and its bets on internation security, magazine of wisdom for philosophical studies, book 09, number 02, 2021, page 795.
15. Amani Aissam, Russia and the use of cyber-power in managing its international relations, p173, on the link:

https://jpsa.journals.ekb.eg/article_200069_efa19d1f2a8f15faf259e9d8822f7d8b.pdf