THE IMPLICATIONS OF THE LACK OF A CYBER-CONFLICT DEFINITION

Luis Carlos AVELLA HUERFANO[♣]

Abstract

This article aims in the first place, to answer why a general definition of cyber-conflicts is needed. To do so, it explores the reasons why it has not been possible to create a general definition for this term and what have been the implications of this lack. Among the causes of not having a general definition for the term of "cyber-conflict" it can be found the lack of clarity and rigor in the use of this term and the definition of other terms related to cyber-space that might be confused with each other. In order to better understand the closest approaches to the meaning and definition of what cyber-conflict is, the first part of this paper exposes several definitions of key terms surrounding the concept of "cyber". The second part of the article shows the relationship between the lack of international organizations that regulate or give guidelines regarding cyber-space and the lack of a universal definition of cyber-conflict. The third and last part presents three relevant cases that demonstrate the recent importance of the cyber-space at the state level, its relationship with cyber-conflicts and how the lack of a universal framework prevents a solution to these type of conflicts. After the analysis, the main conclusion of the study is that a universal definition of the term cyber-conflict is required in order to set a framework that allows the development of regulation measurements towards this new threat that the cyber-space has brought.

Key Words: Cyber-conflict, lack of definition, cyber-space, threat, state level, diplomatic crises, lack of regulation.

INTRODUCTION

Technology has become a fundamental part of the human being, is present in everyone's daily life. The use of internet on different platforms such as computers, tablets and smartphones is becoming more common and this has also produced changes in different dynamics, from the simplest and most daily ones such as social relationships to the most complex ones, such as the way international businesses are carried out, the storage of information, banking transactions, political campaigns and even diplomatic relations. Despite

[♣] Master Student of Peace and Conflict Studies Master Program, Ankara Social Sciences University, Department of International Relations. E-mail: luis.carlos.avella@gmail.com their advantages, new technologies also represent a risk to the safety of people, companies and states through different threats.

These threats have different levels: personal, such as hacking of personal email accounts or social networks and different informatic viruses that affect computers or mobile devices; Corporate level, such as attacks between companies to steal information and / or sabotage the competition; And at the state level, such as the theft and leaking of information between different states to generate diplomatic crises, attacks to damage government websites, hacking and black propaganda to sabotage democratic elections, and even virus attacks capable of causing physical damage on state infrastructures. This last approach will be the focus on the present article.

These new threats the states have been facing in recent years have generated tensions within and between states. Some scholars have called this phenomenon as "cyber-conflicts". However, there is no general definition of this term and often changes the meaning depending on the perspective that is used to analyze the phenomenon. There is also a problem in the use of terminology, since many times academics, researchers and journalists use terms such as cyber-space, cyber-attacks, among others, without rigor and consequently, causing confusion. The lack of a general definition of cyber-conflicts leads to the absence of a general path or policy for all states to end or control these conflicts. For this reason, this paper will attempt to answer why a general definition of cyber-conflicts is needed.

To answer the question, this research work will be of a descriptive nature and a literature review of primary and secondary sources, such as official documents and academic texts, will be carried out. The work will be divided in the following way: first, due to the problem in the use of terminology (cyber-, cyber-space, cyber-attacks), some definitions will be presented that will help to better understand what cyber-conflicts are; then, a summary of the institutions that are working on the definition of the term cyber-conflict will be presented; after that, some cases will be presented to expose the phenomena of cyber-conflicts and finally the conclusions.

1. BASIC DEFINITIONS TO UNDERSTAND WHAT CYBER-CONFLICT IS

These days, when reading the press or listening to the news, terms such as cyber-, cyber-space or cyber-attacks are used without any distinction; although they are related, do not have the same meaning. To have more clarity about their meaning and understand better these terms, some of the most complete definitions of these concepts will be presented and compared.

The term “cyber” according to the Oxford dictionary (2018) is defined as "Relating to the characteristics of the culture of computers, information technology, and virtual reality". For Kleinsteuber (2002) cyber- is a prefix taken from an older word although recent, “cyber-netic”, which has a Greek etymological root; comes from "kybernetike", whose meaning is “the art of navigation”. In Tallinn Manual (2013) it is said that "Connotes a relationship with information technology". As it can be seen in the Strategy on Cyber-Security of Montenegro to 2017 (2013), the term cyber- is referred as "anything related to, or involving, computers or computer networks (such as Internet)". Finally, one of the definitions that explains best what the term “cyber-” is can be found in Finland's Cyber-Security Strategy Government (2013):

> The word ‘cyber-’ is almost invariably the prefix for a term or the modifier of a compound word, rather than a stand-alone word. Its inference usually relates to electronic information (data) processing, information technology, electronic communications (data transfer) or information and computer systems. Only the complete term of the compound word (modifier + head) itself can be considered to possess actual meaning. The word cyber- is generally believed to originate from the Ancient Greek verb κυβερεω (kybereo) to steer, to guide, to control”.

As seen, these definitions have something in common: they consider that the term "cyber" on its own does not have a specific definition, or give any full meaning.

Despite the first impression, the term cyber-space is not a univocal term. Cyber-space, as cyber-culture or globalization, is a term used in different ways, in different contexts and with different purposes. Brunner (2018) describes cyber-space, based on its structure, as "the virtual geography created by computers and networks". Following this, it has been equated to information highways, understood as the common space created in telematic networks. Cyber-space has also been defined as the field of communications constituted by a computer network (El Mundo, 2018).

Hans Kleinsteuber (2002, p.47) presents a more restricted concept of cyber-space to differentiate it from information superhighways. Based on the so-called Magna Carta of the Information Age, of 1994, he characterizes those, among other features, because they are limited in their content by the power of State's Control and the tendency towards centralization and bureaucratization. Cyber-space, on the other hand, would have exactly the opposite characteristics.

In the Tallin Manual (2013) cyber-space is defined as "The environment formed by physical and non-physical components, characterized by the use of computers and electro-magnetic spectrum, to store, modify and exchange data using computer networks". The United Kingdom Cabinet Office (2011) defines it as "An interactive domain made of digital networks that is used to store, modify and communicate information. It includes the internet but also other information systems that support our businesses, infrastructure and services". The Prime Minister Office of Israel (2011) defines this term as "the physical and non-physical domain that is created or part of all of the following components: mechanized and computerized systems, computer and communications networks, programs, computerized information, content conveyed by computer, traffic and supervisory data and those who use such data ".

According to the previous definitions of cyber-space, the following can be said: there is no universal or general definition about the term, each country or author includes or excludes factors within definitions. The most complete definition is the one made by Prime Minister Office of Israel (2011), since it links the physical part of cyber-space (hardware), the virtual part (software, internet) and the human part (the user) within the definition.

In terms of cyber-attacks, the Tallinn Manual (2013) defines this term as "a cyber- operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects". The UK Cabinet Office (2011) defines it as "anything from small-scale email scams through to sophisticated large-scale attacks with diverse political and economic motives. Large-scale attacks may have a number of interrelated goals such as: gaining unauthorized access to sensitive information; causing disruption to IT infrastructure; or causing physical disruption (e.g. to industrial systems)". NATO (2014) defines cyber-attacks as an "action taken to disrupt, deny, degrade or destroy information resident in a computer and / or computer network, or the computer and / or computer network itself".

As for cyber-conflicts, there is really very little that has been researched and written about it, although there are several academic texts and researches that mention the topic, these are not enough and often do not receive the importance they deserve. One of the most complete definitions of this term, given by Henry J Sienkiewicz in his book "The Art of Cyber-Conflict" defines the term cyber-conflict as "the use of computational means, via microprocessors and other associated technologies, in cyber-space for malevolent and / or destructive purposes in order to affect, change or modify diplomatic and military interactions between entities "(2017, p 90). This definition limits cyber-conflicts to the relationship between states, meaning that an attempt to hack a personal email of a student or any worker for the purpose of generating personal tensions cannot be defined as a cyber-conflict, but if the hacking attempt aims to generate diplomatic or military tensions between two states, and it succeeds, it is a cyber-conflict.

Brandon Valeriano and Ryan C. Maness in their book "Cyber-War Versus Cyber-Realities" (2015) wrote about the importance of terminology and the importance of researching and theorizing more on the subject of cyber-conflicts. They also made a summary of cyber-disputes among rival states, like China, the United States, India, Japan, North Korea and Russia from 2001 to 2011, in which it is explained that the attacks between states do not necessarily end in a cyber-conflict: "Only 16 percent of all rivals have engaged in cyber-conflict. In, total, we recorded 111 cyber-incidents and 45 disputes over the period of relations among the 20 rivals "(p, 88). This shows that many times the states allow "small attacks" that they do not consider so dangerous for political and military stability and do not see the need to start a cyber-conflict.

Despite the existence of these definitions and the attempts of several academics to give an universal definition of cyber-conflicts, there is not yet one that is accepted globally and there is, so far, no international organization or authority that covers the majority of countries that are working on this problem.

2. INTERNATIONAL ORGANIZATIONS AND CYBER-CONFLICTS

One of the reasons why there are currently no standardized definitions of terms such as cyber- conflict, cyber-war, cyber-attacks, etc. is the lack of an international authority or organization of a global nature that can set the guidelines, principles, rules and norms on the topics related to cyber-space. In the last 20 years the concern for the ethical, legal, political and anthropological problems of cyber-space has been accentuated throughout the world and worldwide examples are proof of it: the celebration of the Round Table on Cyber-culture, held in the city of Hannover in 2000; the 2000 Infoethics Seminar of governmental experts from Latin America and the Caribbean on "The Right to Universal Access to Information in the XXI Century: The Ethical, Legal and Sociocultural Challenges of the Information Society for Latin America and the Caribbean "; and the celebration of the III International Congress of UNESCO on the Ethical, Legal and Social Challenges of Cyber-space, which took place in Paris on November 15, 2000. However, it was not until the attacks of Estonia in 2007 that the international community realized the real importance of cyber-space and how it could be a risk for the development of relations between states and could represent a danger to the security of every country.

Internally, the states have begun to create measures to face the new problems that cyber-space brings; One of those measures is the creation and implementation of guidelines and / or cyber-security strategies. Many countries so far have their own document regarding this topic; however, the definitions and scope of the strategies are often different. Likewise, the measures and punishments of offenders vary from country to country: these measures are frequently insufficient, since cyber-space has no borders and cyber-criminals often do not reside within the country they affect, revealing the need for establishing international binding strategies and standards on cyber-space.

At a supranational level, the United Nations (UN) created the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GEG). However, as Orcutt (2017) describes, this group that was created to define how the current international legislation should be applied to cyber-space, failed in reaching a consensus in the terminological use. Despite this, they made some progress in the development of some non-binding rules, such as the one that claims that one state should not attack the critical civil infrastructure of another in times of peace. At the beginning of 2017, the GEG did not reach a consensus and did not submit a report to the UN General Assembly. This failure of the UN led to the creation of a new commission that includes both public and private representative as well as academicians that aims to develop a guide of good practices and clarify how to apply international law to new cyber-conflicts. This commission is called Global Commission on the Stability of Cyber-space.

On the other hand, NATO, after a proposal from Estonia, created in 2007 the "NATO Cooperative Cyber- Defense Center of Excellence" (CCDCOE) in Tallinn. The majority of the member countries of NATO participate in this commission and hold regular meetings to discuss progress and problems and to provide solutions. Representatives from different states and academics participate in these meetings. This has been the only international commission that has so far discussed the problem in the definition of cyber-conflict, being a recurring theme in its meetings and publications. One of the problems that have been identified thanks to this commission is that there is very little academic information about cyber-conflict, also a problem in the use of the terms (the use of the term cyber-war instead of cyber-conflict), as well as the lack of researchers working on these issues. Despite the efforts of the CCDCOE, a globally accepted definition of cyber-conflicts has not yet been reached (Herzog, 2011, p.55).

3. RELEVANT CASES

Below there are three cases that demonstrate the importance of terminology and a definition of cyber-conflict and the consequences of not having an international authority that can regulate the cyber-space through the statement of a universal framework. The first case is the attacks in Estonia in 2007, this case shows, among many other things, that the states were not prepared to respond to the threats of cyber-space, and it is from this moment that terms such as cyber-attacks, cyber-war or cyber-conflict begin to become popular in the international arena. Then we have the case of Stuxnet; this case is also relevant since it showed that cyber-attacks not only put at risk information but also can affect the physical infrastructure of the states. Finally, there is the case of cyber-attacks from China to the United States that resulted in major diplomatic crises.

3.1. The Estonia Attacks: On April 27th, 2007, a series of cyber-attacks began, that affected several websites of organizations in Estonia, in the context of a conflict between Estonia and Russia over the relocation of the Tallinn Bronze Soldier, a Soviet monument of the II World War (McGuinness, 2017). The main objectives were the websites of the Estonian Presidency and Parliament, most of the ministries, political parties, three of the most important media corporations in the country and two important banks. The crisis unchained a wave of denial of service (DDoS) attacks; where websites are flooded with thousands of visits that "jam" them and clog the bandwidth of servers. Another type of attack identified was the use of “botnets” for the massive distribution of spam.

The first reaction of the Estonian Foreign Affairs’ Minister Urmas Paet was to accuse the Kremlin of being directly involved in the attacks. However, the Minister of Defense accepted that they lacked evidence to make such an accusation (Traynor, 2007). So far, neither NATO nor the European Commission has found any evidence of any involvement from the Russian government. Only an Estonian citizen with Russian origins has been convicted, who ended up admitting his guilt for attacking the site of the Estonian Reform Party.

The attacks triggered the importance of the issue of cyber-security in the modern militia. NATO undertook political actions after a meeting and a communiqué issued from Brussels in June 2007, which ultimately resulted in the creation of the Cooperative Cyber-Defense Center of Excellence. It has been operating since 2008 and its mission is to become the main source of information regarding cyber-defense (Tamkin, 2017).

What can be seen in this case is that, first, the states were not prepared for cyber-attacks; the efforts of the states have historically focused on strengthening their security and defense, however these efforts only focused on the physical aspect and forgot to reinforce security and defense in the cyber-space. Second, thanks to this case, organizations such as NATO have tried to respond to threats and have begun to investigate and try to define this new problem that states face. Finally, it shows that the lack of an authority or organization to regulate the cyber-space and the difficulty of demonstrating the guilt of an individual, organization or state are the causes that make impossible to punish or implement sanctions against the real responsible of the cyber-attacks.

3.2. Stuxnet, the first "cyber-weapon": On January 2010, inspectors from the International Atomic Energy Agency visiting a nuclear plant in Natanz, Iran, noted that the centrifuges used for uranium enrichment were failing. Interestingly, the Iranian technicians who replaced the machines also seemed amazed (Holloway, 2015). The phenomenon was repeated five months later in the country, but this time the experts could detect the cause: a malicious computer virus. The "worm" - now known as Stuxnet - took control of 1,000 machines involved in the production of nuclear materials and instructed them to self-destruct. It was the first time that a cyber-attack succeeded in damaging the infrastructure of the "real world" (Kelley, 2013).

3.3.

After the attack in Iran, Stuxnet has infected more than 100 thousand computer systems around the world (Zetter, 2014). At first, the worm seemed to be one of the bunch, created to steal information. However, the experts soon determined that it contained code specifically designed to attack Siemens Simatic WinCC SCADA systems that are responsible for controlling the handling of pipelines, nuclear plants and other industrial equipment (Pazulka, 2016).

According to Nakashima and Warrik (2012), the United States and Israel would be behind the creation of this "Worm" and the subsequent attack on Iran. However, there is insufficient evidence to blame a specific agency or individual, and consequently, to generate sanctions.

This case shows that cyber-attacks can also affect the tangible world, and like the case of Estonia, shows the difficulty of punishing the guilty, because although there are many signs of the culprits behind the Stuxnet virus, there is not enough evidence to be able to apply sanctions to the states behind this attack.

3.4. China vs. USA: In early 2010, Google reported that it had detected a cyber-attack from China that had breached the company's security wall and had accessed to its servers. At first, it was reported that the attackers wanted to have access to the email accounts (Gmail) of prominent Chinese opponents, such as Ai Weiwei. Google did not facilitate the investigation launched by the FBI at its headquarters in Mountain View and began a legal dispute with the US security agency to prevent its agents from accessing sensitive company information related to its technical operation (Nakashima, 2013). Time later, it was known that the cyber-attacks against Google and other US companies, in addition of having a nature of industrial espionage and anti-opposition, could have had the main purpose of counterintelligence (Markoff, 2011). Apparently, as described by Zetter (2010), hackers in the service of Chinese state agencies would have launched Operation Aurora to control the information held by US agencies about Chinese intelligence agents operating within the territory of the United States.

3.5.

A few years before this attack, another assault from China managed to violate the defenses of the US military computer system by staying active for almost two years, between 2003 and 2005. That attack, known as Titan Rain, infiltrated mainly private contractors of defense, although it also penetrated the systems of NASA (Thornburgh, 2005).

In June 2015, China hacked the U.S. Office of Personal Management's systems, leaking more than 4 million sensitive records. The U.S. government's only viable response was economic sanctions against companies and individuals (Hirschfeld, 2015).

This final case demonstrates that every state is vulnerable to cyber-attacks, including the United States. It also shows the scope that this type of attacks can have, generating diplomatic instability even in two countries as powerful as China and the United States. Like the two previous cases, this case also demonstrates the impossibility of generating sanctions or demonstrating the guilt of a government, in this case the Chinese government, in the cyber-attacks on the United States.

CONCLUSION

As seen in this paper, there are several factors that have hindered the definition of the term cyber-space and its related issues, such as cyber-conflicts, cyber-attacks, etc., from happening. First, the use of these terms without the necessary academic rigor from states, researchers, journalists, among many others that lead to misinformation and confusion; Second, the lack of research creates an important hole in the field, although there are several investigations regarding this topic, they are not enough to build a strong base of knowledge and some of the existing ones, are not as well appreciated as they deserve to be. Finally, there is a lack of an international organization or authority that regulates cyber-space issues through a universal framework, that can set guidelines, definitions and even sanctions.

While it is important to have a generally accepted definition of several terms related to cyber-space, is the term cyber-conflict which has the greater importance because it directly affects states, as seen with the given examples. Unfortunately, as long as the term does not have a globally accepted definition, it will not be possible to generate guidelines and rules to regulate this phenomenon. Simultaneously, there is a need for an international organization acting as the authority on this matter, responsible of the creation of these guidelines and rules under a global framework and capable of managing and controlling every issue regarding cyber-conflicts. Without the definition and the organization, it will not be possible to regulate and mitigate properly a cyber-conflict and its consequences. This is why it is necessary that the debates about the definition matter and the researches of the cases continue, in order to generate an academic base on which international organizations can support themselves to generate the regulations needed by the cyber-space and eventually, create the authority that is required.

Bibliography

Brunner, J. 2018. Cibercultura: la aldea global dividida. Retrieved from: https://www.researchgate.net/publication/265287580_cibercultura_la_aldea_global_dividida

El Mundo. 2018. Diccionario el Mundo. Retrieved from: http://diccionarios.elmundo.es/diccionarios/cgi/lee_diccionario.html?busca=Ciberespacio&diccionario=1

Finland. 2013. Finland's Cyber-Security Strategy Government Resolution 24 Jan 2013. Retrieved from: http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber--security-strategy.

Herzog, S. 2011, Revisiting the Estonian Cyber- Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, Vol. 4, No. 2: 49-60, 2011. Retrieved from: https://ssrn.com/abstract=2807582

Holloway, M. 2015. Stuxnet Worm Attack on Iranian Nuclear Facilities. Retrieved from: http://large.stanford.edu/courses/2015/ph241/holloway1/

Hirschfeld, J. 2015. Hacking of Government Computers Exposed 21.5 Million People. Retrieved from: https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html

Kelley, M. 2013. The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. Retrieved from: http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

Kleinsteuber, H. 2002. El surgimiento del ciberespacio: la palabra y la realidad en Vidal Beneyto, J. (Editor): La ventana global, Taurus, Madrid, 2002, pp. 47.

University of Oxford. 2018. Oxford Dictionary. Retrieved from: https://en.oxforddictionaries.com/?utm_source=od-panel&utm_campaign=en

McGuinness, D. 2017. How a cyber- attack transformed Estonia. Retrieved from: http://www.bbc.com/news/39655415.

Montenegro. 2013. Strategy on Cyber- Security of Montenegro to 2017 (2013). Retrieved from: https://ccdcoe.org/strategies-policies.html.

Nakashima, E. 2013. Chinese hackers who breached Google gained access to sensitive data, U.S. officials say. Retrieved from: https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html?utm_term=.d72ebcb4c83e.

Nakashima, E & Warrick, J. 2010. Stuxnet was work of U.S. and Israeli experts, officials say. Retrieved from: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.25cd42acad75

NATO. 2014. NATO AAP-06 Edition 2014. Retrieved from: http://nsa.nato.int/nsa/zPublic/ap/aap6/AAP-6.pdf

Orcutt, M. 2017. El nuevo vigilante privado de la geopolítica y el ciberconflicto internacional. Retrieved from: https://www.technologyreview.es/s/8812/el-nuevo-vigilante-privado-de-la-geopolitica-y-el-ciberconflicto-internacional

Pasulka, N. 2016. A Virus Altered the Face of Security in Iran. Retrieved from: http://www.takepart.com/article/2016/07/25/zero-days-stuxnet-iran.

Prime Minister Office of Israel. 2011. Advancing National Cyber-space Capabilities, Resolution No. 3611 of the Government of august 7, 2011 – 2011. Retrieved from:

http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber-/Documents/Advancing%20National%20Cyber-space%20Capabilities.pdf

Sienkiewicz, H. 2017. The Art of Cyber- Conflict. Dog Ear Publishing, (pp. 5-180).

Tallinn Manual. 2013. Tallinn Manual on the International Law Applicable to Cyber- Warfare – 2013. Retrieved from: https://ccdcoe.org/tallinn-manual.html

Tamkin, E. 2017. 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber- Threats?. Retrieved from: http://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber--threats/

Thornburgh, N. 2005. Inside the Chinese Hack Attack. Retrieved from: http://content.time.com/time/nation/article/0,8599,1098371,00.html

Traynor, I. 2007. Russia accused of unleashing cyber-war to disable Estonia. Retrieved from: https://www.theguardian.com/world/2007/may/17/topstories3.russia

United Kingdom Cabinet Office. 2011. UK Cyber- Security Strategy (2011). Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber--security-strategy-final.pdf

Valeriano, B & Maness, R. 2015. CYBER- WAR VERSUS CYBER- REALITIES: CYBER- CONFLICT IN THE INTERNATIONAL SYSTEM New York, NY: Oxford University Press, 2015, 288 pages. ISBN: 9780190204792

Zetter, K. 2014. AN UNPRECEDENTED LOOK AT STUXNET, THE WORLD'S FIRST DIGITAL WEAPON. Retrieved from: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Zetter, K. 2010. GOOGLE HACK ATTACK WAS ULTRA SOPHISTICATED, NEW DETAILS SHOW. Retrieved from: https://www.wired.com/2010/01/operation-aurora/