Arab American University of Palestine- Ramallah

Faculty of Graduate studies

"Cross-Border Cyber Attacks Under International Law"

By

"Yasmin Mazen Mhanna AbuAli"

Supervisor: Dr. Raed Abubadawia

This thesis was submitted in partial fulfillment of the requirements for the Master's degree in International law and Diplomacy

July, 2022

Cross-Border Cyber Attacks under International Law

By

Yasmin Mazen Mhana Abuali

This thesis was defended successfully on 26th, January 2023 and approved by:

Committee members	**Signatures**
Supervisor: Dr. Raed Abubadawia	. ……
Internal Examiner: Dr. Sania AbuAmro	……
External Examiner: Dr. Majd Owda	……

Dedication

I first dedicate this to whom believed in me every time I made a joke or said anything coming from my heart. I dedicate all my work for you, whom stayed with me in my deepest times of my life and for whom laughed and consoled me when nobody understood me, to the person who was by my side even though I gave him a hard time because of my bad mood, to that person who never let go of me and loved me more than I ever thought, for him whom made me believe in life and happiness again. You are the most precious thing in my life and if I have to give my all to someone it would be YOU.

I also dedicate this to my father, the person that gave me the chance to persuade my dreams, the one who supported me emotionally and financially. A big thanks to the button of my heart for believing in me and in my studies.

My mom, my other half and my love, I also dedicate this to you, the person that let go of her dreams just to stand by us. You are an incredible women and and amazing mother. Thank you for always being the greatest mother you are and a father to us when we needed it.

Finally, I dedicate this to my beloved sisters and brother who were always my supporters and partners in life. Thank you for making me feel not just like a big sister but also a second mother to

Fighting is ordained upon you and it is disliked by you; it may well be that you dislike a thing even though it is good for you, and it may well be that you like a thing even though it is bad for you. Allah knows and you do not know.

- (Q.S. Al-Baqarah:216)

Acknowledgements

"And whatever of blessings and good things you have, it is from Allah." (16:53)

I would like to express my sincere gratitude to the Arab American University of Palestine for accepting me as part of their family. I am very happy to be part of the International law and Diplomacy team and being one of the students that seeks to study in their homeland and be a diplomat one, this is why I am grateful to have studied this program.

Further, I would like to thank my supervisor Dr. Raed Abubadawia for always helping me and being there whenever I had questions. He is a very thoughtful professor and I indeed thanks him for all the comments and recommendations on this dissertation. I am also thankful to University and all its member's staff for all the considerate guidance. To conclude, I cannot forget to thank my family and friends for all the unconditional support in this very intense academic year.

Declaration

I, Yasmin Mazen Mhana Abuali student number 202012717, declare that this thesis represents my own work which has been done after registration for the degree of MA in International law and Diplomacy at the Arab American University of Palestine, and has not been previously included in a thesis or dissertation submitted to this or any other institution for a degree, diploma or other qualifications.

I have read the University's current research ethics guidelines, and accept responsibility for the conduct of the procedures in accordance with the University's Committee. I have attempted to identify all the risks related to this research that may arise in conducting this research, obtained the relevant ethical and/or safety approval (where applicable), and acknowledged my obligations and the rights of the participants.

Signature	*Date*

Abstract

Global expansion of the internet has become faster and more expanded .This has led to create a powerful technological revolution which emerges to rise even more over the years. Today, the internet has gathered every actor in the world together from states , individuals ,organizations ,non-state communities ,academia and business. Nowadays ,we see states rely their military power on advanced computer systems and networks which has opened to a new power .Thus ,now we see states trying to use different types of war-fighting such as cyber attacks instead of land ,sea or air .However ,looking at the nature of means and methods of warfare ,we tend to raise the question of the legitimacy of cyber attacks under international law .

However ,applying the rules of IL to technology and cyber attacks can entail a certain difficulty since the characteristics of a cyber attack is not the same as the type of warfare under land ,sea or air .This thesis provides an overview of the most controversial topics in international law and analyses the types of cyber attacks and their legitimacy under International Law (IL) and International humanitarian law.which was divide into three main chapters, an introduction that gives and overview on the main problem, a second chapter that provides a legal framework and a third chapter that focuses on international law topics regarding cyber attacks. Our main objective was to provide a general understanding of cyber attacks and its type as well as the application of IL regarding this matter . Our results had showed that cyber attacks are unlawful under IL and they violate sovereignty and nonintervention as well as almost every single topic in IL such as principle of proportionality and others as well. From a safety perspective, this study emphasizes the need to take into account the impact of these cyber attacks to the safety of a state.

Keywords— *Cyber attacks ,Cyber warfare ,Cyber security, Cyber espionage ,Cyber operations, international law ,international humanitarian law ,states ,non-state actors ,organizations ,sovereignty, non-intervention.*

Table of Contents

List of Abbreviations

IL…….. International Law

IHL……. International Humanitarian Law

EU…… European Union

HRC……. Human Right's Committee

ICC……International Criminal Court

ICESCR…… International Covenant on Economic, Social and Cultural Rights

ICJ……..International Court of Justice

IHRL…… International Human Rights Law

UN……. United Nation

UNGA……. United Nation General Assembly

UNSC…….. United Nation Security Council

ICT……. Information and Communications Technology

FBI…….. Federal Bureau of Investigation

ILA ……. International Law Association

UNOEWG…… The United Nation Open-ended Working Group

UNGGE……. the United Nations Group of Governmental Experts

ITU……International Telecommunications Union

AT&T…….American Telephone & Telegraph Company

INTERPOL……..The International Criminal Police Organization

UNODC…….The United Nations Office on Drugs and Crime

APWG…….Anti-Phishing Working Group

INHOPE…….the International Association of Internet Hotlines

IWF……..the Internet Watch Foundation

IO…… International Organization

NATO……. The North Atlantic Treaty Organization

Chapter 1: Introduction and Methodology.

1. Introduction: Thesis importance and objectives.

Nowadays, we often see humans more interested in the darker side of technology instead of using it for more meaningful matters. It is really controversial how technology can be used to create this delusional effect where humans can step aside back and hide all their evil and cruelty. Either persons, states or organizations the fact does not change it stays the same. With the new technological advancements that we foresee even wars have been changed. The traditional way of going into an actual fight with soldiers and weapons and use the force of the body to reach goals and success has become an old way to win. Now, with the increase development of technological weapons, instead of the kinetic ones like missiles and riffles, now we can use drones and stealth bombers to attacks.

However, the issue is basically in the center of purpose of these new means in a war. The fact that weapons are being used in a more modern and accurate way doesn't mean that the rule changes and they don't have an illegal aspect or immoral sense. It is true that back in the days wars were very pervasive and deadly and the tensity of these wars had led to created a more moral mean to reduce violence and danger, but changing the means and the methods to apply basically the same aim and intention does not mean that there will not be violence or danger, in fact it has been proven how technology have a dark side where it promotes cruelty and a very dangerous reality.

Looking at the importance of technology and internet, we see that the world is being dominated by what its called cyberspace. Nowadays, we see how national governments rely on cyberspace, how the society that is managed by cyberspace wants

to create their own rule. Both governments and society now try to manage conflicts from the laws and judiciary from their own space. The fact that cyberspace creates this dilemma of addiction both parties try to protect it as much as they can. Since the emergence of the internet, both national governments and international system and community try to find regulations and agreements that protects it. We even witness how much can a government try to limit the use of internet and the access to certain information. For example, in China, its government tries to maintain control over what content people can access through internet.

In the U.S also we see how the government limits certain activities like sharing digital data. The idea that cyberspace is now consider as a weapon it leads us to the thinking of how the internet is consider a fundamental key to a states success and power gaining. This is why many states try to implement very advanced security systems to prevent any kind of attack as well as private activities. What makes cyberspace a very interesting field in law and politics and how well it can be used to hide truth and do secret actions. The secrecy of the cyberspace system is incredible that any state can intervene in other states affair without being exposed.

Just like Mike McConnel said, the information that is being managed by a computer network that runs almost every kind of activity a human needs from transportation, banking accounts and transactions can be exposed and threatened in any time from anywhere in the world. [1]It is beyond amazing the fact that there is no need for ships, bombs, missiles or even armies to attack someone or a state without crossing a

[1] Cortada, James W., 'Uses of Computing in the Banking Industry' The Digital Hand: Volume II: How Computers Changed the Work of American Financial, Telecommunications, Media, and Entertainment Industries(New York, 2005; online edn, Oxford Academic, 1 Sept. 2007), https://doi.org/10.1093/acprof:oso/9780195165876.003.0002, accessed 1 Feb. 2023.

single border. This is what makes cyberspace interesting but dangerously fatal if it was used for the wrong purposes.

When looking at the importance of cyberspace in the political world we note that this field has grown to big to have a political significance in the international society. It had become an essential element for norm regulations and political calculus which makes the geopolitical space more important. It is notable that the cyberspace has become a tool for cyberattacks and operations either led by individuals or groups. Cyberspace has become a national and international threat when used to attack a state or a non-state actor. It can create frustration and sophistication if its used to threaten the national security, its economy, democracy or safety.

Researches in this field are considered to be nearly new since for decades the world has been witnessing constant changing. The fact that the internet and specifically cyberspace is new to our century it is important to study the field in every point of view possible, either from a political perspective, law, economy or literature. This research constitutes a relatively new are which focuses on cyber operations and their legality regarding to international law. This field of study has been explained by few researchers since its considered a new topic. One of the major topics to be investigated in this field is cross border cyber attacks and how international law deals with it through its treaties and conventions. This is why our interest in this field lays down in the fact of how this topic is still a new subject to the international law system.

1.1 Introduction to the Issue.

While cyberspace remains an important field to research due to its many advantages, it is also essential to search its consequences when using it for immoral and

unlawful matters. Using cyberspace for malicious means can create conflicts among states and non-state actors. Even though cyber operations haven't yet created major conflict, it is however seen as an enormous threat since it creates vulnerability in any governments system and can expose threats led by terrorist by using their cyber capabilities to destroy anything. When referring to a cyber world, cyber attacks can be different from real ones since blood can't be seen or violence. The force that is used in a cyber operation implies a long term damage rather than a rapid one. The damage that a cyber attack can cause doesn't necessarily be a physical attack rather than a non physical, economic and unsolvable damage.

Because cyber attacks are different from real ones, it is difficult to apply a legal framework on the use of force to them. Even though cyber attacks can have a more major consequences than a nuclear war or comparable to it is arguable on how cyber operation have an actual probable consequence. When referring to cross boarder cyber attacks it is difficult to manage a theory or an argument of whether the law can really explain the legitimacy of cyber attacks since we are not talking about a traditional concept of territorial jurisdiction. The fact that a cyber attacks towards a state or a non state actor is happening, the law has it hard to find legal sources on how to punish the use of cyberspace in an unlawful way. However, this does not mean that technology is immune to the legal system or vis-a-vis.

When talking about attacks and wars in international law we refer to a disturbing and potentially destructive method to eliminate any danger that goes against a state . Using certain types of weapons under IL and IHL is prohibited and by this, states should always stay under the limits of methods and means of warfare .It is to be explained that

under IL certain types of warfare aren't being explained nor analyzed when it comes to their legitimacy like cyber warfares and cyber terrorism, which are technological war acts that may qualify as an armed attack or act or war under international law .Such acts including power grids ,air traffic control systems , banking networks and others are considered as acts perpetrated by state actors and non state actors who are responsible of using such attack without thinking of its danger .

The most disruptive and potentially destructive types of cyber attacks are those that target critical national infrastructure power grids ,air traffic control systems ,banking networks ,etc which may qualify as armed attacks or acts of war under international law. Such acts are characterized as cyber warfare when perpetrated by state actors ,and cyber terrorism when perpetrated by non-state actors. A key consideration in deciding how to respond to such an attack is determining who is responsible ,often referred to as the problem of attribution.

Cyber warfare is a method that allows combatants to fight with ethical and moral considerations from an extreme distance like using drones. [2]Those who use technology to manage cyber attacks far from a real battlefield try to stay away from the horrors of war and its brutality which increases the unnecessary harm ,suffer and collateral damage .However ,the legality of cyber attacks under international law is still unsettled .

According to IHL ,an armed conflict should interpret weapons for the purpose of military actions to combat the enemy ,and its necessary to stop any threat that could lead to a damage or suffering of civilians ,but since cyber attacks doesn’t bring by its nature

[2] Madubuike-Ekwe, J. N. (2021). Cyberattack and the Use of Force in International Law. Beijing Law Review, 12, 631-649. https://doi.org/10.4236/blr.2021.122034

armed weapons the opinion of how to apply IL to cyber attacks is a bit controversial.[3] Cyber crimes from networks espionage to drones is considered as a crime which have created issues to the international society .In its fifth session the UN has issued numerous statements regarding cyber abuse and how technology could affect the interest of a community by disturbing international security and interest) .[4]

Since the Internet has played a significant role in extending states and non-states actors power to the point they use it to attack each other, International law have addressed the issues of cyber attacks ,however it hasn't stated anything about the applicable law for its types .This is why ,this thesis will try to have an overlook and deep analyze about cyber attacks and it's types and how they could lead to breach international law rules and international humanitarian law which can endangers someones life. This topic isn't very much addressed till now ,not many thesis research or doctorates has been made about this matter and its legitimacy under IL .There aren't many researches made about cyber attacks or warfares which is why we seek to answer and fill the gap of the following question: How IL is applicable to cross border cyber attacks by analyzing its norms and principles?. How can the conduct of cyber attacks and warfares lead to a serious breach under IL and IHL?

We also seek to under other question to know whether International law provide cyber security or not. What is the legitimacy of malware? Why international law and norms do little in preventing non state cyber attacks? Are cyber attacks a use of force? Are cyber attacks considered as international threat and international crimes? What

[3] Gervais, M. (2012). Cyber Attacks and the Laws of War. Journal of Law & Cyber Warfare, 1(1), 8–98. http://www.jstor.org/stable/26441233

[4] Khan. A and Ullah, Maseeh and Rehman, Fazal and Ghani, Abdul, Cyber Attacks in International Law: From Atomic War to Computer War (November 3, 2017). Available at SSRN: https://ssrn.com/abstract=3064787 or http://dx.doi.org/10.2139/ssrn.3064787

international treaties sets the rules of cyber attacks and warfare? Do cyber attacks violate the sovereignty of a state or not?

To conclude, the issue of cyber attacks is not whether the law applies to it or not but rather how jus ad bellum and international law rules can interpret it and explain it based on existing rules. In this thesis I will examine the tie-in and connection between cyber attacks and current international law in terms of jus ad bellum and war crimes. First I will discuss the terminology regarding the subject using past and present example cases. I will present the history of cyberattacks and its evolution from the bellum justum doctrine to the current system. Then many notions regarding war attacks and cyber attacks will be examined to determinate whether there is a legality of military action. Everything will be discussed based on cyber operation terms.

1.2 Overview of literature review.

Cyber attacks under international law is still considered a new topic in which states still study to improve their capacities to stop a cyber attack that can endanger the nation security and cause damages whether its economically or politically. Studies in the recent years have been trying to prove how cyber attacks can violate certain aspects of IL. Each author or specialist tries to take an angle from IL point of view and related to cyber attacks or cyber terrorism. What differentiates in this thesis, is that it provides an overall view of many international law topics and analyses it under a cyber context to have a general view of how it breaches the rules and norms of IL. For instance, according to new research, international law is applicable to cyberspace just like any other non cyber activity. It outlines the fact that cyber attacks violates the sovereignty of

a state as well as its political independence which can endanger a state power.[5] This study only shows a cyber point of view in relation to the principle of sovereignty without outlining other principles which still creates a gap because it is important to analyse if cyber attacks breaches all norms of IL or just sovereignty, which is what this thesis will focus more.

Another recent study from Haataja has argued that cyber attacks are overview regarding information ethics and how it is considered a use of force which violates international law. It has emphasized that cyber attacks can be looked in an ontological view by embodying anthropocentric and materialist conception of violence. He had described how an state is viewed as an entity and how cyber attacks increases violence between states. This study tries to bring an interesting angle of how cyber attacks are a form of force and how they make violence even more.[6] However, it does only outline this aspect in a very deep analytical information and not other aspects of international law which still makes a gap of where else does cyber attacks also violate in terms of international law rules.

Another Report of the Study Group co-organized by the University of Bologna, University of Milan and University of Westminster [7] had also made an intensive deep report outlining different aspect of international law but from an arbitrary point of view. They have explained cyber attacks in terms of sovereignty, non intervention, state responsibility, international humanitarian law aspect as well as international disaster law.

---

[5] Moynihan, H. (2019b, December). The Application of International Law to State Cyberattacks Sovereignty and Non-intervention. Chatham House: The Royal Institute of International Affairs. https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf

[6] Haataja, S. (2017). Cyber Attacks and International Law on the Use of Force: an Informational Approach. https://research-repository.griffith.edu.au/bitstream/handle/10072/365740/Haataja_2017_01Thesis.pdf?sequence=1&isAllowed=y

[7] Report of the Study Group co-organised by the University of Bologna, University of Milan and University of Westminster. (2021, February). INTERNATIONAL LAW AND CYBERSPACE. https://www.esteri.it/wp-content/uploads/2021/12/UNIBO_Applicazione-dei-principi-della-Carta-delle-Nazioni-Unite-nello-spazio-cibernetico.pdf

They have explained how cyberspace and cyber attacks can violate these norms by proposing an Italian specialist overview. The difference between this thesis and this report is that I took various important topics in international law and I brought a more personal analyses based on treaties, articles and UN Charter rather than just focusing on a one topic. Plus, the report had emphasized more on state comments and providing countermeasures.

Moreover, another study entitled *Cyberwarfare and International Law* had outlined Cyberwarfare as a non dramatic humanitarian consequences which hasn't led yet to a human tragedy and had exterminate if new weapons and methods of Cyberwarfare can be compatible with the obligation of international humanitarian law and the moral responsibility of a state.[8] This study had focused more on the outcomes of a Cyberwarfare and how they violate IL in circumstances where it causes serious breach. What is different in this thesis is that I focused more on the violation of cyberattacks under international law whether the attacks are simple or complex rather than focusing more on the cyber attacks in times of complexity and war time.

1.3 Methodology

This thesis provides different types of methodology that helps us reach a conclusion to our answer. The main method was the use of analytical and descriptive methods which allowed me to study cyber attacks under international law and use our literature review and already information that helped us to do an analyses on how cyber attacks can be a breach to a state sovereignty and political independence. The thesis also provides an information bases of different cyber attacks types and their meaning and

[8] Melzer, N. (2011). Cyberwarfare and International Law. https://www.files.ethz.ch/isn/134218/pdf-1-92-9045-011-L-en.pdf

how are they a breach to IL. I also have answered our questions based on different key topics of international law and I applied them to cyber attacks and how are they implied in the system.

Thus, I have used many case studies like the Stuxnet Virus cyber attack and how it was a breach of IL. So I implied real case studies and example to profound the analyses based on a qualitative method. In some parts of the thesis, a doctrinal method was used by gathering data and information about cyber attacks through treaties and legal documents. I have described treaties and doctrines as well as important manuals like the Tallinn Manual to explain how certain IL topics like the non intervention and sovereignty are applied to cyber attacks and how the law applies to it. In doing so, this thesis will provide a mix of existing information and a personal analyses by going deeply into each point and relating it to the law.

1.4 Thesis overview and limitations.

The aim of this thesis is to determinate whether cyber attacks can be a violation of IL and how the norms and principles of IL are applied . It will essential to discuss the matter of non-intervention and sovereignty and how it is related to force and the issue. Thus, there will be some concluding remarks and some views towards the issue upon the final analysis based on a profound descriptive and analytical basis with the apply of a fundamental legal research. Chapter 1 gives an introduction and overview to the thesis by discussing the issue and research questions. Chapter 2 discusses the historical background of the concept of war and how it led to the creation of cyber war and crimes. It discusses cyber attacks and its types as well as cyber weapons and by who are they used and when.

Chapter 3 provides a law enforcement view on cyber attacks by discussing important legal sources like the Tallinn Manual and Article 2(4) of the UN Charter as well as ICJ and ICC along with the UN and regional organizations and the view of customary international law. Chapter 4 is where the analyses is provided by dividing this chapter into sections and focusing on different IL topics like the principle of sovereignty, non intervention, proportionality and others. This chapter provides the answer to our main question and finally concludes what the thesis is about by analyzing and discussing how really cyber attacks are a breach to IL just like Kinetic wars.

This thesis only provides an analyses on how cyber attacks are a violating of IL in terms of cross board between states and not between individual or organizations. The thesis only focuses on cross border cyber attacks between states and how they breach the rules of international law and can endangers the security of a state. The reason why our thesis scope only focuses on states is because we want to analyse different aspects of IL and how are they applied on cyber attacks that happens between states in peace and war time.

Chapter 2: The concept of cyber attacks and its types.

2.1 Historical background

2.1.1 Understanding the concept of war.

It has been analyzed during the years that humans have different changing behaviour that could create some sort of a conflict environment due to many reasons. War has been an ubiquitous feature of a human condition. Almost every nation had to seek wars to reach the outcome of what they wanted. It is nearly impossible to find nowadays a nation without an armed force, this is because force has become an essential tool for

defending ones nation and ideology. If we want to look at the history of war, we should go back 1900 years ago where wars were the bloodiest in history. In fact, one of the most bloodiest and aggressive wars by man made was the second world war which was the biggest catastrophe of all times. [9]

If we want to understand cyber wars it is important to begin with war itself and understand it more. When analyzing the meaning and aim of war it is indeed important to outline that wars are actually human made towards another human being directly regardless of the way. However, sometimes these who try to seek war as a solution aren't being acted as solo bur rather by another commander or agent. Understanding war isn't about knowing the reason of why someone wants to kill but rather the policy of what their actions implement.

To begin with, wars have been conflictous because of religious, ideological, independence and ethical matters. For example, we have seen that decades ago, the church[10] was a main reason for war because they wanted to apply a one faith base. We have heard about the Thirty Year War between Catholics and Protestants for religious matters and domination.[11] The Napolian waged wars[12] are also another example, where his troops fought for glory. Also, the civil war in Russia after 1917[13] which aimed for revolutions. And if we want to look before 1000 BC we constantly can note that wars

[9] Paret, P. (1971). The History of War. *Daedalus*, 100(2), 376–396. http://www.jstor.org/stable/20024009

[10] When wars began to show, it was related to the Churchs beliefs that a state has a right to defend itself, and its peoples, from an act of aggression, though the manner in which it does so will still need to be bound bound certain principles.

[11] The war between Catholics and Potestants for religious matters lasted from 1618 to 1648, starting as a battle for states that formed the Holy Roman Empire. However, while the war of 30 years was being envolved, it had became more religious and more about governance in Europe.

[12] Napoleonic Wars were between Napoleonic France and shifting alliances of other European powers which were fighting over the hegemony of Europe which constituted a war of 23 years.

[13] The Russian Civil War made Russia tore apart for a 3 years period from 1918 and 1921 because of the emergence of opposition against the Bolsheviks after November 1917. These groups included monarchists, militarists, and, for a short time, foreign nations.

have been going on since ever. The first ever war listed was the Campaign by King Scorpion (I) against King Taurus in 3250 BC which focused on the concentration of power in later prehistoric Egypt.

Looking at the reasons of war, we can constant that wars have been the result of hate, domination, fear, power mostly, prejudice, religion, territory and so forth. One of the main reasons was the competition for resources or territories. Le Blanc explains that even today's warfare are almost the same as those of tens of thousands of years ago, due to the same causes, tactics and same attitudes. [14]Accordingly, John Kekes defines war as the hostile connection by the means of armed forces in which nations, states or rules carries it, against another power.[15] He explains the fact that war is being seen as an organized violence by voluntary intentions in which armed forces plan to act and use weapons aiming at the enemy. According to him, war can take many forms and it can be seen as a terrorist act or a way of resistance depending on the circumstances. [16]

War is also defines according to the LORANOW[17]. The concept is being understood from a long range, cross policy perspective which is defined as an occurrence which happens to imply lethal violence between two social groups that pursue the same political goal but which results in fatalities. At least one of these groups is being organized by an authorization power that leads the belligerent groups to reach

[14] Gleditsch, N. P., Pinker, S., Thayer, B. A., Levy, J. S., & Thompson, W. R. (2013). The Decline of War. International Studies Review, 15(3), 396–419. http://www.jstor.org/stable/24032901

[15] KEKES, J. (2010). War. Philosophy, 85(332), 201–218. http://www.jstor.org/stable/40666542

[16] KEKES, J. (2010). War. *Philosophy*, 85(332), 201–218. http://www.jstor.org/stable/40666542

[17] The Long-Range Analysis of War (LORANOW) is a project that began in 1988 at the University of Colorado, Boulder, to develop the concept and understanding of war and peace in recorded history. LORANOW is considered an interdisciplinary research program based on historical data sets, mathematical models, and microcomputation to examine long-range (LR), cross-societal patterns of war and peace. It builds on past and present projects which have developed and statistically tested conflict data bases and new mathematical theories of international conflict using probability models.

the goal for them. [18]

If we want to look at the history of war be need to go back 400 BC, reading about the Greeks war and their battles like the Battle of Melos, the Battle of Carthage in 149-46 BC. War crimes didn't start in the 20th century they were long before even though it started as abuses and minor violence till it develop to become deadly crimes and massacres. It is true that at that time these minor abuses weren't called war crimes however, they qualified as war crimes due to the nature of the events. According to the Greeks, war crimes were considered as actions with no morality. People began using war as a way to defend their ideologies and religions like the Peloponnesian War[19]. The Athenian people wanted to defend their realism ideology and it was not considered a moral matter but rather a legal condition[20].

Even though war was not considered a war crime itself back then, now it is considered a much more thing. The concept of war has been developed to become a political instrument. It has been associated with political intercourse that carries many means. [21] According to Clausewitz[22] the nature of war comes from violence and the emerge to win as a passion. His first consideration is that war has a political aim because it has a cause and a purpose which determinate its conduct. He concluded that

---

[18] Cioffi-Revilla, C. (1996). Origins and Evolution of War and Politics. *International Studies Quarterly*, 40(1), 1–22. https://doi.org/10.2307/2600929

[19] The Peloponnesian War was between the period of (431–404 BC) whichwas an ancient Greek war fought between Athens and Sparta and their respective allies for the hegemony of the Greek world.

[20] Schu, A., & Cadenza Academic Translations. (2017). WHAT IS WAR?: A REINTERPRETATION OF CARL VON CLAUSEWITZ'S "FORMULA." *Revue Française de Science Politique (English Edition),* 67(2), I–XVIII. https://www.jstor.org/stable/26607592

[21] Hater, D. A., & MacCuish, D. A. (2005). A History of War Crimes and Their Consequences. *In The International Criminal Court: Why We Need It, How We Got It, Our Concern About It* (pp. 1–24). Air University Press. http://www.jstor.org/stable/resrep13871.7

[22] Lindell, J. (2013, May 3). Clausewitz: War, Peace and Politics. E-InternationalRelations. https://www.e-ir.info/2009/11/26/clausewitz-war-peace-and-politics/

war act as an operation in a battlefield which can be performed in a brilliant way but they are considered worthless if the aim wan not political itself. He argues that war is always a political matter which makes sense since all powerful countries tries to manage political activities through war itself. [23]

If we want to look at the evolution of war historically, we need to study the type of policy and the goal of war. For instance, in the 17th and 18th century , it began with an absolutist state policy which created a dynastic conflict and the consolidation of boarders. In this century it was used mercenary and professional arms such as the use of firearms that are defensive which had led in result the regularization of taxation and borrowing. In the 19th century the type of policy changed to a nation state by using different military techniques such as railways and telegraphs with rapid mobilization which led to the expansion of administration and bureaucracy. In contract, when looking at the 20th century even the goals of war changes. Policies began using multinational states, which resulted in the use of massive arms and firepower to mobilize the economy. Nowadays with the evolution of technology , bloc policy are being used, ideological conflicts are the main purpose, the use of nuclear weapons and elite armies and the development of cybernetics to use cyber wars resulted in a military industrial complex .[24]

2.1.2 The evolution of technology and its link to wars historically.

Throughout history, we have seen technology grow faster and for the benefits of

---

[23] *George Dimitriu (2020) Clausewitz and the politics of war: A contemporary theory, Journal of Strategic Studies, 43:5, 645-685*, DOI: 10.1080/01402390.2018.1529567

[24] Kaldor, M. (1999). New and old wars: Organized violence in a global era. *Stanford, Calif: Stanford University* Press.https://dl1.cuni.cz/pluginfile.php/654678/mod_resource/content/1/kaldor%20-%20old%20and%20new%20wars.pdf

human who wants to create a world that is more developed which can improve more the life of others. Societies have been constantly change especially when it comes to the ambience and environment of the war. The weapons that have been used in war have been changing over the years which changes the policy of war but not the object of it. Before 400,000 BC we see war weapons beginning by using spears specially in Germany, or hunting as a way to get to the enemy. Later on, bows and arrows were replace, and the use of boomerangs in 23,000 BC. Years later, in 5300 BC, horses were used an instrument in warfare which were an important transportation back then[25]. Subsequently, in the Bronze age we see the evolution of metal daggers and the creation of swords as weapons.

Afterward, weapons wee more linked with the evolution of technology which led to the creation of gun powders[26] which was invented in China and then the creation of the first rocket known as the fire arrow[27] in the era of 1000 AD. While technology was being more improved, the weapons used in war became more aggressive with created a more deadlious war environment. In 1600 AD, firearms technology were being created such as hand cannons. Latter, matchlocks, rocket artillery, submarines began to be used in battles specially in the American Civil War from 1861 to 1865. also, revolving guns, gatling guns, iron clad warship, and submarines were used in anger.

It was until the first world war, technology was used in a more modern way which

---

[25] Rice, J. (2020, May). ANIMALS IN ANCIENT GREEK WARFARE: A STUDY OF THE ELEPHANT, CAMEL, AND DOG. https://mospace.umsystem.edu/xmlui/bitstream/handle/10355/78092/RiceJenna.pdf?sequence=1&isAllowed=y

[26] Gunpowder was known to be as a mixture of saltpeter (potassium nitrate), sulfur, and charcoal. This technology was dicovered by the Chinese in the 9th Century and it had been used fist as medicinal purposes and then was applied to warfare

[27] Fire Arrows - The First Explosive Rockets. (n.d.). A Brief History of Rockets. https://wasfun.weebly.com/fire-arrows---the-first-explosive-rockets.html

played a huge role in carrying out the war and it made it much bloodier and protracted. High explosive shells were been used, and first tanks were introduced by British army. In 1914, the US came up with the Manhattan project which attempted to build its first nuclear bomb under the direction of J.Robert Oppenheimer[28]. In 1945, war was declared in Hiroshima, Japan[29] which effectively ended the second world war and the nuclear weapons era began more strongly. Henceforth, in 1952 the US also engaged in the Marshall Island project[30] were they first tested a hydrogen bomb and used X-rays which created a more stronger bomb than the one used in the Hiroshima war. Afterward, ray guns and lasers, tasers, were used in warfare. It wasn't until the 20th century when technology was presented in a more aggressive way, high energy laser was created, weapons that fires million rounds a minute, airbone lasers , neuroscience and most important and impressive cyber attacks. [31]

Technology has been an important contribution to war specially when it comes to the equipment used, it has played a significant role that changed the means and the methods of warfare. Today, we see technology more lethal and precise. With the creation of weapons of mass destruction and high technological laser, satellite weapons that are used to attacks individuals with their exact location. However, the desire to minimize the risk of a potential real war and the loses that can be faced either economically, military or other, the 21st century is introducing a more developed way to

---

[28] History.com Editors. (2022, April 19). Manhattan Project. HISTORY. https://www.history.com/topics/world-war-ii/the-manhattan-project

[29] Britannica, T. Editors of Encyclopaedia (2022, September 12). atomic bombings of Hiroshima and Nagasaki. Encyclopedia Britannica. https://www.britannica.com/event/atomic-bombings-of-Hiroshima-and-Nagasaki

[30] K=1 Project research in the Marshall Islands | K=1 Project. (2020, August 6). https://k1project.columbia.edu/news/k1-project-research-marshall-islands

[31] Marshall, M. (2019, March 12). Timeline: Weapons technology. New Scientist. https://www.newscientist.com/article/dn17423-timeline-weapons-technology/

engage in a war without being deadly or use enormous weapons that cost millions of dollars. This is why, the expand of technology is creating a more easy and reliable method for warfare which is the use of cyberspace and cyber technology in general.

2.1.3 The start of a new era: cyberspace.

The era of technology became much wider with the spread of development and progress in our world. With the development of cybernetics, the world has become much closer and easier to connect regardless of the circumstances. When talking about technology we refer to a complicated ambience yet a modern way to live. Technology has created a space where people can connect, talk, engage no matter the distance. With cyberspace being a major essential to our lives, it has became one of the most essential tools in the international community either for economy engagement, politics, sociology or even governing. The term cyberspace first has been discussed in the Ancient Greek time which meant governor, pilot or rudder[32]. The term was created and mentioned by Danish Susanne and Carsten Hoff in 1960s[33]. The word was refereed back then to the installations and images which were called sensory spaces. It meant the art of sensing behaviors of humans and materials in space.

Cyberspace was first defined in the 1980s, by William Gibson and Neuromancer[34] which refers to the state of hallucination which is experienced by operators daily in a

[32] Malik, J., & Choudhury, S. (2019, March). Cyber Space- Evolution and Growth. : East African Scholars J Edu Humanit Lit ISSN 2617-443X (Print) | ISSN 2617-7250 (Online) | Published by East African Scholars Publisher, Kenya. https://10.36349/easjehl.2019.v02i03.005

[33] Lillemose, J., Kryger, M., Madsen, K. V., Stasinski, R., Gabrielsen, S., Steiwer, L., Joung, N., Ciel, S. M., Stasinski, R., Madsen, K. V., Ravini, S., Schlaegel, A., Drønen, L., Steiwer, L., Gabrielsen, S., & Korpak, H. (2015, September 22). The (Re)invention of Cyberspace. Kunstkritikk. https://kunstkritikk.com/the-reinvention-of-cyberspace/

[34] Merchant, B. (2013, April 24). Why William Gibson Invented Cyberspace. https://www.vice.com/en/article/78834d/why-william-gibson-invented-cyberspace

legitimate way, it is described as a graphic representation which contains data from computers all over the world. This term had became popular as a synonym for computer network and Internet. Nearly every domain in the world from literature, law or art has a definition for cyberspace. Many official government sources had emphasized the meaning of cyberspace. Also, in DoD, cyberspace[35] has been defined as a global domain that consists of technology information that infrastructures and residents data.

Technically, cyberspace is a doing that was first developed as a result of the first computer in 1946[36]. when computers became a mass production and was commercialized in 1950, that's when cyberspace became an important matter in people's life. The link between computers and cyberspace had grown in people's daily life as an important way of connecting together. Cyberspace had became a major tool with the help of the internet which was an essential system to build a wide network service. The internet became an international network that connected every single country in numerous fields. According to some definitions, the term cyberspace has been linked to physical infrastructures like mobile devices, computers..etc , it has been linked to computer systems and networks as well as data and information.

Cyberspace had strongly linked to represent human existence nowadays. The development of the internet created an interaction between humans with has been liked to human behaviour. Cyberspace had became a tool that controls humans activity. It has been linked to online social behaviour like buying online good, online activism

[35] Air Land Sea Space Application (ALSSA) Center. (2022, January 1). DOD Cyberspace: Establishing a Shared Understanding and How to Protect It. https://www.alsa.mil/News/Article/2891794/dod-cyberspace-establishing-a-shared-understanding-and-how-to-protect-it/

[36] Kanellos, M. (2007, July 25). ENIAC: First computer makes history. ZDNET.https://www.zdnet.com/article/eniac-first-computer-makes-history/

behaviour like protesting in something, but most interesting and dangerous behaviour is the one linked to cybercrime behaviour like engaging in illegal intrusion, electronic theft, espionage and more.

When it comes to law, cyberspace has been also a subject in local and international laws. In order to maintain a secured space for people, it is important to maintain the security of cyberspace by regulating the law since its part of a social order and behaviour. Many countries began to establish a legal system regarding cyberspace and law regulations which focuses on the protection of the critical information infrastructure either by securing the physical entities or the logical security of infrastructure. By enhancing the protection and security of cyberspace, it allows the fight of cybercrimes. For example, countries like the U.S have established many legal acts that regulates the security of cyber space like the 1966 Freedom of Information Act, the 1974 Privacy Act, the 1984 Computer Crime, the 2000 Government Information as well as many others.

2.1.4 The beginning of cyber crimes.

Cybercrimes had been a way of using internet in a malicious way in order to attack and destroy either systems, information or networks using the internet to commit crimes. Since cyberspace has been emerging each day, many cybercrimes has been realized. Cybercrimes had been recognized as a very enormous harm and a new way of committing crimes without being faced with the other opponent. Since cybercrimes had become very recognized around the world, many researches have been conducting new legislation. Because of the fast development of technology and cyberspace, cybercrimes had become more diverse.

The definition of cybercrimes has constantly developed according to the law

institutions that are considered an important source in international law and local law. For instance, the National Institute of Justice of the U.S in 1979 had referred to cybercrimes as a crime committed with the help of a compute which forms a white-collar-crime[37]. In 1995, the UN Manual on the Prevention and Control of Computer Related Crime[38] had also linked cybercrimes to illegal acts such as fraud, forgery and unauthorized access. In the 10th congress of the UN on the Prevention of Crime and the Treatment of Offenders[39], had also discussed that cybercrimes have illegal behaviour which is directed by electronic operations that targets the security of a computer system. It is also a ways of distributing information with a network in an unauthorized way. Other legal sources such as the Council of Europe's Cybercrime Treaty[40] included that copyrights infringement is also an aim of cybercrimes.

With the spread and development of technology, nowadays the new crimes often are related to cybercrimes which are not like the traditional ones since they often take place in cyberspace. Criminals in this era, have excellent computer skills that helps them commit crimes by only invading someone else information system. Cybercrimes can be discussed as in various types. For example, cybercrimes can happen when a crime does not harm directly the system, when the system doesn't really crash but has wrong result, when the resources of the system are stolen or when the system is broken down and that's when the user cannot use the system at all. For example, the first

[37] Computer Crimes | Office of Justice Programs. (n.d.).https://www.ojp.gov/ncjrs/virtual-library/abstracts/computer-crimes-2

[38] Affairs, H. A. D. S. F. C. U. N. (1994). International review of criminal policy.United Nations Digital Library System. https://digitallibrary.un.org/record/162804?ln=en

[39] Tenth UN Congress on the Prevention of Crime and Treatment of Offenders "Crime and Justice: Meeting the Challenges of the Twenty-first Century" Vienna, Austria 10 - 17 April 2000 . view more on: https://www.unodc.org/congress/en/previous/previous-10.html

[40] See more at: https://www.coe.int/en/web/cybercrime/home

cybercrime that has occurred was in 1971, when John Thomas Draper who was a computer programmer tricked the American Telephone & Telegraph Company (AT&T) telephone network so they can give him free calls by using toy whistles found in Cap'n Crunch cereal boxes.[41]

In 1981, Ian Murphy had also committed a cybercrime [42] by hacking the AT&T network and changing the internal clocks which were responsible of the billing rates. Other crimes were committed, such as computer viruses, like in 1982, Elk Cloner had created a computer virus which infiltrated his school system[43]. In 1989, there was also a ransomware which attacked the attendees of the World Health Organization's Acquired Immune Deficiency Syndrome (AIDS) conference by given them floppy disks to lock down their computers. [44]

When it comes to law, cybercrimes aren't being really considerate in traditional laws. However, most countries and some international organizations have created some legislation against cybercrimes. For example, Canada has an International Cybercrime Research Center that belongs to the Simon Fraser University. The U.S has the CERT Division and the U.S Department of Justice Criminal Division Computer Crime and Intellectual Property Section which is ruled by the government. India has an Asian School of cyber laws. England has a Crime and Security Research Institute. Other countries like China have a Cyber Security and Crime Research Center which belongs

[41] Van Vuren, S. van. (2021, August 26). The History of Cybercrime. Itcareerswitch. https://itcareerswitch.co.uk/the-history-of-cybercrime/

[42] The History of Information Security: A Comprehensive Handbook. A de Leeuw, K.M.M. A Bergstra, J. 9780080550589. https://books.google.ps/books?id=pQBrsonDp6cC. 2007, I Elsevier Science

[43] Awati, R. (2021, December 8). Elk Cloner. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/Elk-Cloner

[44] Gillis, A. S., & Lutkevich, B. (2021, December 17). ransomware. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/ransomware

to the Chinese government, as well as the EU which has a Data Protection and Cybercrime Division.

2.2 Terminology: war, cyberwarfare , cyberwar and cyber operations

When talking about war and its difference between an actual war and a cyber war we need to pay attention to many details and differences since both have different contexts regardless of the similarities. In this actual table, we will discuss the differences between an actual war, a cyber war Vs cyber warfare and what are cyber operations.

Concept	Definition	Types	Example Case
Actual war	According to Clausewitz, an actual war is the act of using violence to compel an opponent to do a will with a political intention and moral mean. It is an act that is characterized by destruction on an extensive scale.[45]	Colonial war, Proxy war, Religious war, Range war, Cyber war…etc	First World war, Second World war, Cold war..etc

[45] VON CLAUSEWITZ, C. (1976). On war.

Cyber war	According to many, a cyber war in a war where the attack and the defense is happening in a network system which aims to destroy the enemy's network and weaken its function. its main aim is to destroy another country's computer network by implementing an act of virtual violence.	Threatening, Attacks…etc	The Stuxnet Virus which was a worm that attacked the Iranian nuclear program.
Cyber warfare	Cyber warfare is the act of using techniques and tactics that are used to attack an opponent and	Denial-of-service attacks, Computer viruses and worms, Pishing, malwares etc…	Morris worm 1988

https://www.usmcu.edu/Portals/218/EWS%20On%20War%20Reading%20Book%201%20Ch%201%20Ch%202.pdf

	damage its network system, it does not imply the protraction or violence but rather the procedures.		
Cyber operation	Is the act of using cyber space capabilities and computer networks to perform a cyber attack operation or the act of protecting from a cyber attack by operating certain strategies.	Cyber security	VPNS

2.2.1 Cyber attacks

Cyber attacks aren't that different from cyber warfare or cyber crimes in terms of context. According to Richard Clark, a cyber attack[46] is the act to infiltrate into another country computer network or the same country to cause a damage or disruption. Michael Hayden also defines cyber attacks as the intention to destroy another country

[46] Smith, J. F., Walt, S. M., Bayyenat, A., Dormandy, X., Lynn-Jones, S. M., & Smith, J. F. (n.d.). Richard Clarke on Cyber Threats: Defense is Key. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/richard-clarke-cyber-threats-defense-key

computer network, however the definition does not extend to non-governmental attackers. Martin Libicki extends the definition to a digital attack[47] that causes computer network system to appear normal but in fact it creates an issue by damaging it. Further, Tallinn Manual Group[48] gives another definition that explains the fact that cyber attacks are cyber operations that causes injury, death, damage or even destruction of property. The effects that a cyber attack can have can lead to major consequences.

To understand more about the reasons and consequences of cyber attacks, it is important to understand who does it in the first place. Hacking a system network and stealing data can be made more commonly by states which they try to steal data from other states, and this process is called computer network exploitation. Hacking also can be made by corporations which try to steal intellectual property data, or by individuals for the purpose of identity theft. However, it does not mean that an individual cannot attack a state or vis-a-vis.

When analyzing cyber attacks, it is important to look at the two types of cyber attacks that takes places. First, the external cyber attack which happens when hackers try to hack an organization system frequently, resulting in damages to them. It happens when poor security is being confronted. The second types, is the most dangerous one and it is the internal cyber attack which is happened inside an internal source which cause grave damage to the company or organization by stealing information and exchange them with a foreign user for money. [49]

---

[47] Burns, M. (1999). Information Warfare: What and How? https://www.cs.cmu.edu/%7Eburnsm/InfoWarfare.html

[48] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. doi:10.1017/9781316822524

[49] What is a cyberattack? | IBM. (n.d.). https://www.ibm.com/topics/cyber-attack

A study made by the National Cyber Security Centre, 2016 entitle *"Common cyber attacks: reducing the impact"*[50] has showed that hackers tend to use any kind of mean to reach their goal by using cyberspace and open sources like social media. They will use techniques and tools to access an organization information by getting into their security system. They tend to find errors where they can hack the system easily.

Cyberattacks can be seen in many types and forms, they target a network or system which is made by a third party and the attacker is known as a hacker. Cyberattacks comes with many negative effects resulting in data loss, manipulation, breach, etc. A cyber attack tends to damage an organization reputation and target financial sources. It is to believed that since Covid-19 cyberattacks have increased much more notable because of the lack of cybersecurity. There are many types of cyber attacks which can affect an individual, company in a large scale depending on the situations. The most comment type of cyberattacks are ransomwares, others are known a "*Man in the middle attacks, Enial of service attacks (DOS and DDoS), SQL Injection attacks, DNS Tunneling, Zero day exploits and attacks, Password attacks, Drive by download attacks, Cross site scripting (XSS) attacks, Rootkits, DNS spoofing or poisoning, Session hijacking, URL manipulation, Cryptojacking and Inside threats."*

2.2.1.1 Most common types of cyber attacks and case examples.

In this section, it will be discussed only the two most common types of cyber attacks that can be found in cross border cyber violation in order to understand more about how these two types can violate the norms of IL which will be discussed further

[50] Wermser, D. (2017, November 15). Security of IoT Cloud Services - A User-Oriented Test Approach. https://www.academia.edu/73600677/Security_of_IoT_Cloud_Services_A_User_Oriented_Test_Approach

later on in the next following chapters.

2.2.1.1.1 Malware-based attacks (Ransomware, Trojans, etc.)

When taking about a malware attack we refer to it as a malicious attack to the software of a computer. When using this type of attack, the attacker performs malicious activities with codes that are interchangeable. The attacker can apply this attack using different forms like viruses, trojans, worms, spyware, ransom-wares, etc. Many of the cyberattacks on internet are malware based attacks, including a nation-state cyber war, a cybercrime, fraud or even scams. For example, when using Trojans hackers tend to steal classified information from government networks, or encrypting data of a users computer so the user cant have access to it. [51]

One of the most recent ransomware examples is the Ryuk ransomware [52]which appeared in 2018. it is believed that attackers from this ransomware are being operated by a Russian cyber criminals known as Spider Wizard. It is believed that they do not attack directly but rather download a malware into a computer first. The Ryuk has been listed in 2020 as the most dangerous ransomware attack. They always tend to attack large companies. A report in 2020 from the Crowd Strike Global Threat has reported that over 12.5$ million dollars had been demanded by this virus.

In 2019, Ryuk made a cyber attack against several newspapers in the U.S. newspapers from LA Times, Wall Street Journal, NYT and San Diego were delayed because of a malware attacks that hit the system of Chicago-based tribunal which is

[51] Lee, W. (2019). Malware and Attack Technologies Knowledge Area Issue 1.0. https://www.cybok.org/media/downloads/Malware__Attack_Technology_issue_1.0.pdf

[52] Ryuk - What is Ryuk Ransomware? (n.d.). Malwarebytes. https://www.malwarebytes.com/ryuk-ransomware

responsible for the production and printing process of various newspapers. The attack was made outside the US and the extension link was assigned at the end with an ".ryk". The Ryuk ransomware is considered of the top targeted attackers by the U.S.[53] Also in 2020, another Ryuk ransomware had targeted Universal Health Services (UHS) in the U.S by shutting down the system. As a result, productivity was a common type of loss with a 55% , 34% of data and 17% of financial loss. [54]

2.2.1.1.2 Pishing attacks (Spear pishing, whaling, etc.)

The second most common cyber attacks is pishing attacks which consists of a tricking method that a hacker uses to steal money by sending fake funds to attackers. One of the tricking method that attackers use also is electronic messaging suck as emails and providing links that could contain worms and viruses that takes the user to a malicious website that is controlled by the attacker. Pishing is one of the cyber attcaks that is consider a hybrid attack because it is combined by social engineering and technological aspects too. [55] Phishers always make a plan before targeting a system, they begin with a warning message and many people get fooled by the message because of lack of awareness of society which makes phishing easier. After a warning message, they send a link which consist of hacking the system. The main reason hacker use this method is for financial gains as well as other gains like social. Their motive for phishing could be many, but mostly is stealing banking credentials like credit card details such as

---

[53] Hanel, A. (2022, March 18). Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware. crowdstrike.com. https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

[54] UHS Hospitals hit by Ryuk ransomware, forced to shut down systems. (2020, September 29). 2020-09-29 | Security Magazine. https://www.securitymagazine.com/articles/93482-uhs-hospitals-hit-by-ryuk-ransomware-forced-to-shut-down-systems

[55] (PDF) Phishing Attacks and Defenses. Available from: https://www.researchgate.net/publication/296916234_Phishing_Attacks_and_Defenses [accessed Aug 15 2022].

CVV numbers.

Of the most historical example to this type is the 1996 phishing attack that targeted America On-Line known today as AOL, which is to be considered one of the largest Internet Service Provider in the U.S. Hackers tried to access the password of the AOL user. Another example, can be set through the Hillary Clinton presidential campaign in 2016 which was targeted by phishers. The only thing that the hacker did is send an email to Podester's gmail account in order to disclose his login credentials with a warning message to change the password. So in this case the hacker used social engineering techniques to make the cyber attacks easier without any fail. However, the simplicity of the attack does not necessarily mean that it could be legal. It is still considered an unlawful act. [56]

2.1.3.3 Case examples on recent state cyber attacks

Because of Covid-19 in 2020, cyber attacks had initiated strongly because of the lack of social communication that made societies stay at home because of the international health problem which occurred after Covid-19. States cyber attacks had increased from 2020 till today a lot which cause a cyberspace insecurity internationally. Attacks began to became more clear in the latest 2021 which was caused by individual hackers and then it began more between states. For example, in November 2021, Robinhood a stocking trading company was attacked by a hacker which gained access to more than 7 million customers causing data loss and economical loss. At the same year some hackers had access to the FBI Law Enforcement Enterprise Portal which

[56] Gupta, B. B., A.G. Arachchilage, N., & E. Psannis, K. (2017). Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions. https://arxiv.org/ftp/arxiv/papers/1705/1705.09819.pdf

claimed to be part of the Department of Homeland Security.

In December 2021, a cyber attack by a Russian Group had made a ransomware attack on an Australian CS energy company which was attributed to the Chinese government by the Australian media. In the same year, some Chinese hackers had violated U.S defense and technology firms. Also, another attack was made by hackers that targeted Southeast Asian governments which were linked to the Chinese state. In 2022, cyber attacks became more explicitly, for instance, in January several cyber attacks were made like attacks on Israeli medias like the Jerusalem post which included threatening messages, or the cyber attack on the Ukrainian government which attacked several governmental computers.

Moreover, another cyber attack was made against the International Committee of the Red Cross which was attributed to researches based in Iran. In February, a Russian state sponsored actor hacked U.S defense contractors which filtrated sensitive date. Also, at the same month, a Pakistani group conducted a cyber espionage on an Indian military and diplomatic corps. Another attack was made by the Russian government to the Ukrainian defense ministry which was a DDoS attack. In 2022 and because of the Ukrainian-Russian war, many cyber attacks were made specially by Russia which is know by attacks through cyber means. In April, a group that had connections with Russian GRU, targeted several Ukrainian media organization.

In April, a Russian Hacker had targeted the Costa Rican Ministry of Finance which resulted of an economic loss and leak of data. At the same month, a campaign by Russian hackers targeted diplomats and embassies from France, Poland, Portugal and other countries with a pishing email. In May, a Russian attack from type DDoS targeted

the Ministry of Defense and the National Health Institute. In July, Russia was blamed for a cyber attack that targeted a Ukrainian media company. In September, Russia had targeted the UK intelligence agency M15 with a DDoS attack. In October, some Russian hacker took responsibility for hacking a U.S state government website which include Colorado, Kentucky and Mississippi as well as an attack to major U.S airports by pro Russian hackers. Another attack was made in the same month by pro Russian group which targeted the Bulgarian website because they betrayed Russia by supplying weapons to Ukraine. The attack targeted the presidential administration, the Defense Ministry, the Interior Ministry, the Justice Ministry, and the Constitutional Court.

2.3 Cyber threats and weapons.

Cyber attacks are becoming an intelligent way to cause disruption to a state with less cost. Unlike tradition attacks, cyber ones are usually more deniable are more sophisticated since they put a lot of pressure on both sides, forcing the target onto the defensive with a constant threat. Threats through cyber attacks are more aggressive in a way that the damage is outstanding but without blood or human loss. When it comes to law, it isn't a very difficult situation in a way that law hasn't provide effectiveness against cyber attackers because it is difficult to track them because of cross-border activities. Cyber crimes are really becoming more outstanding nowadays, the nature of conflict is changing between states and non state actor.

Cyber threats are becoming a more expected war than conventional ones which we see on land, air or by sea. Since the submergence of cyberspace, cyber threats has become more expanded in a cyber battlefield beyond the geographical boundaries that we usually know. The danger about cyber threats is usually the attackers are that

involved with. It has been noticed that many cyber threats and attacks are operated by non state actors like terrorist groups which tend to target advanced countries. In some cases, states do not attack directly and clearly, instead they hire terrorist or criminal to target other states, which makes it difficult to determine the source of the attack. However, if an attacks was attributed wrongfully against a state without any proven acts this could escalate into a tension and result in an escalator response between two states who either have bilateral relations or not.

Since cyber space has become a main interest to the international community, the same applies to cyber weapons. The fact that a cyber attack can escalate into a cyber war or cyber warfare it is important to know what kind of cyber weapons are being used in these kind of operations. Cyber weapons are considered instruments of harm that acquires human power and technological one. With the advance of technology, weapons have been developing and are more evolving than conventional weapons because of their much faster pace.

In the cyber world developing a weapon does not need to take a years to develop, instead it could be ready in days or even hours. One of the most outstanding examples is the Stuxnet attack on the Iranian Nuclear Facility. A cyber weapon has a political, security and legal consequences. It could be defines as a computer code that is used for threatening or causing physical or mental damage either to systems or persons. These weapons are considered as devices that can lead to a critical infrastructure damage to the program, the data and the information of a relevant system. Cyber weapons can be used to spy, threat or attack. They come in a variety of packages like malwares.

The advantage of using cyber weapons or the reason of why they are becoming a

better option when going into a war is because they are more efficient and less expensive. An attack using a cyber weapons is much more faster and the damage could be worst. The fact that these weapons are less noisy is a plus because an attack can be made without making it too obvious for the enemy to know. Also, what makes it even a better option is because of law attribution which makes attacker go under cover easily without any fear. These weapons are now been considered the weapons of the 21st century because of their difficulty to track and be identifies. This is why states are becoming more active in developing cyber weapons.

According to an Indian study in 2021 by Maj Gen Mallick, titled : " *Cyber weapons- A weapons of war?"*[57], an analysis was conducted about how cyber weapons are considered as a conflict between national and non-national. They are weapons that are used with the help of technological information system in order to cause damage, harm to equipment or people. The characteristics of these weapons is that it can do an action from a very far distance with an accuracy and efficiency that allows to minimize risks and loss including big financial costs. Further, they make military planning much easier since telecommunications are easier. Also, what makes it special is that it buys time for policymakers to make an action.

On the other side, cyber weapons can have disadvantages since it can rise tension between nation states and other actors. When realizing cyber weapons, unexpected effects might happen. If a state wants to grant some power it must have offensive capacities, but when using cyber weapons a state can have cyber defense without necessarily having offensive capability. In contemporary warfare, cyber operations are

[57] Mallick, M. (2021). Cyber weapons- A weapon of war? https://indianstrategicknowledgeonline.com/web/Cyber-Weapons-A-Weapon-of-War.pdf

now consider a must for states. A state needs to acquire cyber weapons to stay active and snatch the initiative when its needed.

When looking at the legal aspect, cyber weapons require illegal actors or states. It would be considered as an illegal action or an act of war if it was performed by an agent during peacetime. It is know that International law is applicable to conventional wars, but when it comes to cyber warfare there is a difficulty in determining what is applicable to it since the problems lays is sovereignty and loyalty. Since international rules and agreements set the rules for the law of war, many experts have reached a conclusion where it also applies to cyber domain.

The use of cyber weapons in a potential war can have consequences specially if it was during peacetime. Many countries have acknowledges the use of cyber weapons like the U.S against Iraq and Syria. The main problem is that cyber weapons aren't being regulated by the law till now even though many nations view them as weapons of war and they view it as weapons of mass destruction that can cause many destruction.

2.3.1 The Stuxnet cyber weapon.

The Stuxnet cyber weapon [58]is considered one of the first weapons evaluated since 2005. it was uncovered in 2012 by the U.S and was used against Iran. The Stuxnet is considered a malicious computer worm that was used as a cyber attack by the U.S and Israel in order to slow Iran’s nuclear program. The worm had cause centrifuges to explode but eventually it got spread around the world and it created a fear that It could potentially be a destructive weapon. This worm was created specially to attack Iran

[58] Ivezic, M. (2018, January 22). Stuxnet: the father of cyber-kinetic weapons. CSO Online. https://www.csoonline.com/article/3250248/stuxnet-the-father-of-cyber-kinetic-weapons.html

directly, however the same worm can be used for other purposes by manipulating computers and causing enormous damage that could many people. However, regarding the law using the Stuxnet worm did not qualify as a self defense weapon according to the law of armed conflict because it has to be under the context of an initiative arm conflict and a significant damage like the loss of a life.

A study was made whether the worm was considered as an act of force or not. According to Hataaja on his study of : " Stuxnet and International Law on the Use of Force: an Informational Approach", the concept of force is within the Article 2(4) of the UN Charter[59], and it was argued that under international law violence involves a state of kinetic weapons to damage a property or kill someone within another state. The Stuxnet was a case arguable by the law since the worm cause non material harm, therefore the law does not give account to non material ways in which states can be harmed.

2.4 Nation state cyber attacks Vs Non-state actors cyber attacks.

States tend not to attack directly by using a computer war instead the cyber happens through the nation state that has some sort of a license to hack since they work for the government to target other governments, individuals, or organizations to access data and information. These group are omnipresent which means that are mostly hidden to the public and they are aligned to the government. Any hacker that works for the government well knows how supportive they should be and the risks that he/she is taking. The thing about nation state attackers is that they are not afraid to get caught or punished because they are already with the side of their country. They have strong links with military, state control and even a high degree of technical skills.

[59] U.N. Charter art. 2, para.4.

The process of picking an attacker for a nation state is not that easy. They can be considered according to the language, their social media account, or their skills in espionage, propaganda and defamation. Once picked, they have the support from the state either with resources, members or any kind of force they need. Nation state actors are highly motivated by nationalism. They can gain secrets by espying on other nations by cyber means and methods. The thing about nation state actors is that they don't own up for their actions, they never acknowledge any claim or suspect which makes them difficult to track or trace.

Unlike nation state actors, non state actors act more present but without reveling their identities. They can be identified as artificial names or characters that can engage in a cyber attack just like nation state actors. They can act like cyber militias like when it happened in the Estonia war in 2007[60] when volunteers took part of the cyber conflict. Non state actors either attack individuals and organizations or they directly attack a state resulting in web defacement, or leaking of confidential information or engage in national security and military affairs. When it comes to the law, non state actors are to be held responsible unlike nation state actors who work for the government[61].

The international law rules and regulations provides states protection from non state actors that commit cyber crimes from the territory of another state. A state is not responsible for the conduct of a non state actor that causes malicious crimes to another state because of a territorial link. It can only held accountability if a crime occurs within

[60] McGuinness, B. D. (2017, April 27). How a cyber attack transformed Estonia. BBC News. https://www.bbc.com/news/39655415

[61] Sigholm, J. (2013). Non-State Actors in Cyberspace Operations. Research Gate. https://www.researchgate.net/publication/310827486_Non-State_Actors_in_Cyberspace_Operations#:~:text=Employment%20of%20such%20non%2Dstate,will%20likely%20reshape%20future%20warfare.

the state, unless it was proven to be a link between the state and the non state actor. In that case, the state can be held responsible specially if there was an international wrongful conduct that had occurred which can be attributed to the state.

2.5 When are cyber attacks usually used: war or peace?

When dealing with cyber attacks, it is normally unknown the exact time when a cyber attack will occurs, and the reason why is because the nature of cyber attacks are more hidden and anonymously operated by attackers that are usually known as hackers. An individual can operate on its own or by the consent of the state in a specific time because of political reasons. An attack could never occur without being studied well and knowing the possible results that a cyber attack can create. It is known that cyber attackers like to be the head of news and specially when there is a war invoked. They usually appear either in time of war by making a plot action or in a time where it is not expected. Many cyber attacks have occurred in military action just like the cyber attacks used by Russia when invading Georgia or the political cyber espionage by the NSA programs[62] which were reveled by Edward Snowden as well as other examples like the state-backed economic cyber espionage during the era of President Xi Jinping's when visiting the U.S.A.[63]

Usually cyber attackers like to attack during peacetime more than war time and the reason why is because it's least expected and states are less prepared for a cyber attack. For instance, in 2012, the U.S and Israel have been targeting Iran by cyber attacks to

[62] Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA. (n.d.). https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

[63] Ide, B., & Huang, J. (2015, September 18). Cyber Hacking Looms Over Xi's US Visit. VOA. https://www.voanews.com/a/cyber-hacking-looms-over-chinese-president-visit-to-us/2968967.html

target the Nuclear Program of the state which resulted in real damage[64]. Also, Iran had targeted Saudi Aramco in 2012 by creating a virus which targeted more than 30,000 Saudi Aramco. Moreover, North Korea had also targeted in 2014 at Sony.[65] China had also been active in cyber attacks on code sharing site GitHub in 2014[66]. An important point to outline is that not always state initiate cyber attacks, also criminals that are considered as hackers or extremist can conduct such attacks such as the attack by an individual against Russia by hacking the TalkTalk company.[67] Also, states do not always need to attack other states, it can attacks individuals, corporations or private companies.

By looking into an international law point of view, it is quite complicated since cyber attacks that happen in peacetime needs a lot of effort to improve if they are considered war attacks or not. It an attack occurs during a war time there is no doubt of it's illegal status under international law if it causes damages to civilians and their objects. However, in peacetime in usually different since the attacks suddenly happen and particularly if they cause mass causalities. If we want to compare between these two, we can partially say that cyber attacks during military can be considered in some cases legitimate specially if concluded that they were used in a defensive mode, but in peacetime wouldn't be considered the same thing since there is no motive to initiate an

---

[64] Nakashima, E., Miller, G., & Tate, J. (2012, June 19). U.S., Israel developed Flamecomputer virus to slow Iranian nuclear efforts, officials say. The Washington Post, National Security. https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

[65] Perlroth, N. (2012, October 24). *Cyberattack on Saudi Oil Firm Disquiets U.S.* The New York Times. https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

[66] New Chinese Cyberattacks: What's to Be Done? (2015, April 10). ChinaFile. https://www.chinafile.com/conversation/new-chinese-cyberattacks-whats-be-done

[67] BBC News. (2018, November 19). TalkTalk hack attack: Friends jailed for cyber-crimes. https://www.bbc.com/news/uk-england-stoke-staffordshire-46264327

attack so it would seem that the cyber attacks was initiated by malicious consent. So by that being said, we can conclude that cyber attacks are usually more used in peacetime because of the large process of discovering who did it and why which can be difficult to detect the origin of the attack and can create also more damage to the target state or individual because it is initiated in the least expected time where the state is not prepared or would take much time to respond back.

Chapter 3: Law enforcement and cyber attacks.

3.1 Customary international law and cyber attacks.

Customary international law[68] is one of the important sources of international law that is derived from general practices as law. Practices that include customary law can be derived from military manuals, national legislation and case law. It is often accepted as a part of international law which refers to *opinio juris*. It is considerable binding upon all states and it is applicable to tribunals and international courts. [69] Customary

[68] The customary international law is an important legal source under international law, it has become an essential matter to discuss if an international law rule is not defined or has the difficulty to correspond to a legal matter. In 1950, the International Law Commission had listed several important sources that takes form of evidence for this specific law such as: treaties, decisions of national and international courts, national legislation, opinions of national legal advisors, diplomatic correspondence, and practice of international organizations.
[69] Derived from the ICRC, found at: https://www.icrc.org/en/war-and-law/treaties-customary-law/customary-law

international law is considered a form that generates the practice of states which is followed by them as a form of legal obligation. Customary international law is usually found in multilateral and bilateral treaties which is taken by states either through international organizations like the UN or by decisions of international courts or domestic ones as well as national legislation and other sources like diplomatic and administrative decisions.

The customary international law if defined in Article 30 of the International Court of Justice which defines it as a legal body that prohibits activities made by states which are not codifies or written down. It is used when states together engage in a particular behaviour which needs opinio juris. [70] This particular law itself is considered as a human law because it was established after mankind. According to the supreme court opinion, the customary international law was founded with the consent of the world. [71]

It is convenient to say that customary international law is considered and old source in which generates rules to be binding to all states. It is not a written source but rather a rule of customary law upon cases and circumstances. To have a customary international law it must have two essential elements. One, it must be a consistent state practice. Two, there needs to be opinio juris. According to the ICJ, in order to bring customary international law to the area, the states practices must be settled and the states must feel that they have a legal obligation to require a rule. [72]

To create a new rule of customary international law, these two elements must be

[70] https://guides.law.sc.edu/c.php?g=315476&p=2108171

[71] J. Paust, J. (1990). Customary International Law: its Nature, Sources and Status as Law of the United States. Michigan Journal of International Law. Retrieved August 23, 2022, from https://repository.law.umich.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1638&context=mjil

[72] (North Sea Continental Shelf cases, ICJ Reps, 1969, p. 3 at 44)

present, which means that the practice alone isn't enough, but also the opinio juris must be present two. For example, in the case of the SS Lotus (1927)[73], a rule couldn't be created without the actual opinio juris. Also, the Advisory Opinion on Nuclear Weapons (1996), the rule couldn't be created because there was no practice.[74] By that means, opinio juris is the belief that an action has been carried out because of legal obligation, meaning that an act must have a legal advisory opinion from experts or higher courts or organization to bring a legal justification to a matter. While state practice is more objective meaning that the state must have a legal obligation and conscience to perform a practice.

3.1.1 State practice to cyberspace and attacks.

As mentioned above, the customary international law has to comprise with two important elements, one of them is the state practice which is seen in the actions of states and their omissions. The state practice can also be seen by statements made by representatives in an international for a or through a state's domestic law and judicial decisions which deals with international relations. For example, in the North Sea Continental Shelf cases between Libya and Malta,[75] the Court had explained that customary international law should be looked into the state practice in this case. A state practice is important because it has the consent of a state and their sense of obligation to act.

According to the ILA Report, several elements need to be found in order for the

[73] The SS Lotus case was a conflict between France and Turkey on a high sea in 1926. the conflict arises in the question whether turkey violated the international law when the turkish courts had exercised jurisdiction over a crime that happened in a french national. The court decided in 1927 that turkey did not violate the law. Read more on the case at:https://ruwanthikagunaratne.wordpress.com/2012/07/27/lotus-case-summary/

[74] See more at the ICJ page at: https://www.icj-cij.org/en/case/95

[75] Continental Shelf (Libya v. Malta), 1985 I.C.J. 13 (June 3); http://www.worldcourts.com/icj/eng/decisions/1985.06.03_continental_shelf.htm

state practice to be counted in customary international law and take it into consideration, one of them is the most important one which refers to the type of conduct by a state and which one counts as state practice.[76] Second, in order for an action to be count as an state practice, it shouldn't only be physical acts but also verbal acts are counted and the reason why is because verbal statements sometimes have more power and influence that those that are physical, when an authoritative representative gives a verbal statement over a matter or case it can influence in the case and count as an action too because it includes opinions and plans that are connected to a right consent of a state. Every diplomatic, policy and press statements as well as official manuals and comments by governments and court decisions are considered as a state practice.

However, for a verbal act to be considered as an state practice it should be made in public and not in private. And w hen we say, public it does not necessarily mean to the whole world but at least the states that are concerned should be informed verbally which is why internal memorandum for example is not considered therefore as an state practice or confidential opinions of governments and even a secretly bugging diplomatic premise. The act can be considered an actual state of practice if it was made in public and legally justified. Moreover, another important point to outline is that acts that are not made on behalf of a state like acts of individual or corporations do not count as state practice even-though if they may be directly involved in a rule or opinion and they encouraged and influence the state to make a certain behavior. Only states and governmental bodies can perform a state practice.

Another point to highlight, is that those activities of territorial governmental

[76] INTERNATIONAL LAW ASSOCIATION LONDON CONFERENCE (2000); FINAL REPORT OF THE COMMITTEE STATEMENT OF PRINCIPLES APPLICABLE TO THE FORMATION OF GENERAL CUSTOMARY INTERNATIONAL LAW. Found at: https://www.law.umich.edu/facultyhome/drwcasebook/Documents/Documents/ILA%20Report%20on%20Formation%20of%20Customary%20International%20Law.pdf

entities within a state which do not enjoy separate international legal personality cannot count as a state practice unless it was ratified by the state. Even international courts and tribunals are not really considered as an state practice because they act individually on their own even if they derive their authority from states. On the other hand, intergovernmental organizations are considered a form of a state practice because it has the participation of states. For example in the Reservations to the Genocide Convention Case the ICJ took into account the practice of UN secretary general and those of national chancelleries. [77]

When it comes to cyberspace and activities, it is important to note that since cyber attacks and operations are new to the world, still many works has to be done and there are many efforts to develop customs on this subject. It is important to imply that customary international law applies to cyberspace and attacks because it has the necessarily elements of state practice and opinio juris like the efforts of the Tallinn Manual which will be discussed latter on. Some state practice in cyber attacks matter have been made. For example, the U.S has made many efforts in this area like setting its view on the application of international law to cyber activities in the Koh's 2012 speech and the U.S submission to the 2014-2015 UN GGE which both are considered as state practice. The U.S has also made other state practices in this matter like discussing and presenting view publicly in its Law of War Manual. Also, the a UN report in June 2013 is considered as an state practice because it is written by experts that have opinions of authoritative intergovernmental opinions. The report had conclude that international law

[77] Berman, Sir Franklin, 'The International Court of Justice as an 'Agent' of Legal Development?' in Christian J. Tams, and James Sloan (eds) The Development of International Law by the International Court of Justice (Oxford, 2013; online edn, Oxford Academic, 2 Jan.), https://doi.org/10.1093/acprof:oso/9780199653218.003.0002, accessed 5 Feb. 2023.

applies to cyberspace in particular the Charter of the UN.[78]

3.1.2 Opinio Juris to cyberspace and attacks.

Opinio juris is another essential element in customary international law. It means an opinion of law or necessity which is often referred to the Latin phrase: *opinio juris sive necessitatis*. Opinio juris is important to establish a legally binding custom, on the opposite of a state practice which has an objective obligation, opinio juris detonates a subjective obligation on behalf of a state which is bound to the law. For instance, the international court of justice in its Article 38(1)(b) ad reflected that for the custom to be applied it must be accepted as law. For instance, in the case of Nicaragua the ICJ had explained that in order for a new customary law to be applied it must have both elements including opinio juris which is very important. States must behave in a conduct where they should believe that their practice is obligatory and apply the subjective element which is opinio juris sive necessitatis.[79]

Also, in the North Sea Continental Shelf Cases, overthought after the convention came into force and the state practice was in favour of the equidistant, it was not deducted the necessity of opinio juris which means that both the subjective and objective element is necessary for a custom to be applied. Opinio juris is not just an individual element it is reflected through the practice of states just like in the Asylum Case where the court held that Colombia failed to prove the existence of a new custom because there was the absence of consistent and uniform usage. Also in the Nicaragua Case the opinio juris was also reflected as well as in omissions specially in acts where it

[78] Wrange, P. (2014). Intervention in national and private cyberspace and international law. International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi, (Leiden: Brill/Nijhoff, 2014) 307-326. https://www.diva-portal.org/smash/get/diva2:778433/FULLTEXT01.pdf

[79] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), ICJ judgement. See more at: https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

was done by a following belief that the state is obligated by law to act. Even in the Nuclear Weapons Case the court held that the GA Resolutions can be important to establish a new custom rule by the emergence of an opinio juris even if the resolutions are non binding which can help to establish a new rule.

In cyber space context, the application of international law to cyberspace has become really relevant in the past few years specially since cyber operations have been rose and carried by states. Customary international law has been developed in the context of cyberspace specially after the publication of the Tallinn Manual which is being discussed till now to become a new form of international treaty for cyber international crimes. Since before we have seen many state practices and opinio juris in relation to this matter. For example, France, Iran, Brazil, Israel, Korea, the UK and U.S have published sophisticated documents that clarify how international law applies to cyber space which is a form of an objective state practice. Other states, have expressed their interest even if in an distant discreet matter. Some have participated in the UN Group of Governmental Experts (UNGGE) and UN Open-Ended Working Groups (UNOEWG).

State practices and Opinio juris had been seen in cyberspace from long time ago specially b China, the U.S and Russia. The first public statement about the application of international law to cyberspace was made by the U.S in 1999 which discussed the Assessment of International Legal Issues in Information Operations, which was published by the Department of Defense's Office of General Counsel. Also, China had clarified several times ts views on the application of international law to cyberspace which included opinio juris which result in the construction of customary international law. Also, one of the most outstanding examples for new

customary international law which includes opinio juris is the Tallinn Manual which was a NATO Cooperative Cyber Defence Centre of Excellence major research project in 2009 to examine the public international law governing cyber warfare and the project included several international group experts.

By that being said, the customary international law and its main elements like opinio juris are now being more seen in the context of cyberspace specially through the Tallinn Manual which will be discussed further more in the next following section.

3.1.2.1 Applicable sources of law as part of customary international law: The Tallinn Manual.

The Tallinn Manual which was published in 2013, is considered one of the first manuals and resources for cyber warfare under international law. This manual is an academic no binding work from experts and a team of legal scholars that tried to bring an explanation and rules for cyber warfare. It was requested upon NATO even though it does not reflect it nor its members. Followed by this manual another one was released in 2017 which discusses cyber operations. [80]

The first manual entitled: "*Tallinn Manual on the International Law Applicable to Cyber Warfare*" discusses international law legal principles and how they are applicable to cyber warfare. The second one entitled: *"Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations"* [81]covers cyber operations and which can escalate to a war and it addresses topics in international human rights law as well as others like law of air and space.

[80] Ginsburg, T. (2017). INTRODUCTION TO SYMPOSIUM ON SOVEREIGNTY, CYBERSPACE, AND TALLINN MANUAL 2.0. AJIL Unbound, 111, 205–206. https://www.jstor.org/stable/27003730

[81] Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations (Michael N. Schmitt gen. ed., 2017).

The Tallinn Manual 1.0 discusses both jus ad bellum and jus in bello both in the context of cyber activities that occurs as a level of force. It is an important source that can relate cyber attacks in different fields of law such as international human rights law and telecommunication law. The manual emphasizes topics such as cyber operations between states, cyber attacks to an enemy command or a control system. It is to be noted that the manual is also used not only for international armed conflict but also a non international armed conflict. The manual examines the fact that there is no direct treaty that addresses cyber warfare because states practice regarding cyberspace or related have opinio juris that is considered sparse. [82]

Further, the manual provides discussion on how both jus ad bellum and jus in bello applies to cyber warfare and operations and how it is applied. The words and phrases that the manual provides has legal and military means such as its definition to the word attack which defines it as a cyber operation against an entity. The first manual addresses cyber warfare in regard to legal terms such a sovereignty, jurisdiction and state responsibility.[83]

Since the manual was written by experts of international law and legal scholars who are expert in the domain, the manual is considered an important reference and source where everything that a specific treaty has not explained, the legal scholars discussed it. Since the Tallinn manual had approached a humanitarian regard, it is essential to note that the its reasonable to adopt the IHL rules to cyber armed conflict since the context of cyber attacks can directly aim civilians and properties that could be

[82] Schmitt, M. (2013). Short form citations. In Tallinn Manual on the International Law Applicable to Cyber Warfare (pp. Xiv-Xx). Cambridge: Cambridge University Press.
[83] IBID, 21

affected because of military targeting because of cyber attacks. [84]

The Tallinn manual is considered important not because of it was a work done by experts but because the context of the manual provides a guide for situations regarding cyberspace and cyber attacks. The manual itself specifies points related to the Petersburg Declaration of 1868[85], the Geneva Conventions of 1949[86] which can apply to cyber space. Many experts have given comments about the manual, saying that it is the first manual that shows points about the law of war in cyber context. [87]

Important topics were discussed in the manual such as the fact that cyber attacks can lead to damages, deaths and destruction. If a cyber attacks was used in times of peace it could be interpreted as a sign of use of force or an armed attack. If the attacks was used in times of war it could lead to another interpretation which leads to self defense. An example, can be given about the Stuxnet attack on Iran which was indicated as an act of force because it was aimed directly in a time where there was no direct conflict between the U.S and Iran. The virus had aimed to target the nuclear program of Iran as part of an attack in a peace moment. [88]

Others topics were discussed in the manual whether a computer can be considered as a legal weapon or not. The legal scholars and experts have explained the fact that computers are indeed weapons that can cause damages to the targeted enemy or a civil

---

[84] IBID, 21
[85] The Declaration of Saint Petersburg is the first formal agreement prohibiting the use of certain weapons in war. To see more, visit: https://ihl-databases.icrc.org/ihl/full/declaration1868

[86] The Geneva Conventions and their Additional Protocols are international treaties that contain rules about limiting the consequences and effects of war. They protect civilians who do not take part in the fighting (civilians, medics, aid workers) and those who can no longer fight (wounded, sick and shipwrecked troops, prisoners of war). To see more, visit: https://www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm
[87] IBID, 21
[88] IBID, 21

population. Also, those who use the weapons which are defined as attackers or combatants of cyberspace. Since the attacks are made anonymously and low profile, its hard to know who is behind the attack which makes it difficult to state whether the law can punish them or not because in an armed conflict, a combatant needs to be distinguished from a civilian and if he/she isn't distinguished and cant be know it won't be possible to apply penalties to them unless their identities are exposed. [89]

Furthermore, it is arguably to note that the manual itself is not a treaty between states which makes it hard to be binding no matter the situation. Since it is not a treaty and states aren't part of a convention related to it, even in armed conflict its difficult to apply the manual as a legal source and legitimate one to states. However, since the manual was written by experts that are considered worthy trust to the international community and refers to other international law binding treaties, the manual can be taken as a serious reference when an cyber conflict is active. By that means, the manual is enhanced academically which makes its credibility even higher.

3.1.2.2 International trends or efforts to combat cybercrime

Since the 20th century, the international community has been quite active regarding cyberspace and its security. From 2015 till now, it has been noticed many activity regarding cyber crimes and cyber security. For example, in 2015 India had declared at the United Nations General Assembly WSIS+10 Meeting[90] that there needs to be an international convention that addresses issues related to cyber crimes and cyber security. China had also declared its opposition against cyber operations and that states should

[89] IBID, 21

[90] The World Summit on the Information Society (WSIS) is a UN event that discusses the implications of the emerging information society. In 1998, the International Telecommunications Union (ITU) made a resolution to develop the emerging information society and utilize Information and Communications Technologies (ICTs) to bridge the global development divide.

not accept any negative behaviour related to cyberspace and had also agreed to conduct a universal standard to fight cybercrime. Also, the UN came up with resolution (A/RES/70/2370) on the *" Developments in the Field of Information and Telecommunicatios in the Contexte of International Security"* which noted that cyberwar and cyberwarfare may be considered a topic under IHL.[91]

Russia had also asked the UN to create an international treaty that could serve states to deal with cyber attack as mentioned earlier before. In 2016, we foresee much more engagement from states, for instance in January 2016, the World Internet Conference was organize in China and it was discussed the fact that people need to have protected online services. In February of the same year, president Obama had established a Commission on Enhancing National Cybersecurity. In October, a new proposal for a Geneva Convention on Declaration for Cyber space had also been proposed by Judge Stein Schjolberg. [92]

In 2017, a new book has been introduced called: *" The History of Cybercrime"* which presents information from the UN, INTERPOL and other organizations. At the same year there was a suggestion to make a Digital Geneva Convention that will allow protection to civilians from nation-state attacks in time of peace. China has came up with a document title: *" International Strategy of Cooperation on Cyberspace"* to

[91] International humanitarian law and cyber operations during armed conflicts: ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019. (2020). *International Review of the Red Cross, 102*(913), 481-492. doi:10.1017/S1816383120000478

[92] A Geneva Convention or Declaration for Cyberspace A global framework on cybersecurity and cybercrime, and a contribution for peace, security and justice in cyberspace By Judge Stein Schjolberg, Norway,1 and Professor Solange Ghernaouti, Switzerland. Found at: https://www.cybercrimelaw.net/documents/Article_on_Geneva_Convention_or_Declaration_for_Cyberspace.pdf

develop a system of international rules and create safeguarding cyber security norms. Another book was released also in the same year title: *" Cyber Attacks- Prevention-Reactions: The role of States and Private Actors"* that discusses the main questions about cyberspace under international law. As well as the book of : " Cyberkriminaliet" published in Norway which consists of the Council of Europe Convention on Cybercrime, the Chairman's Report and the Third Pillar for Cyberspace which is a draft of the UN Treaty on an International Court or Tribunal for Cyberspace.

Moreover, another proposal for a Geneva Convention for Cyberspace was present at the Pan-European Conference. In October at the UNODC conference, there was a proposal suggested for a UN Treaty on fighting online child sexual abuse. In 2018, judges and prosecutors from the EU and the EJTN[93] held a seminar to address problems of jurisdiction and international cooperation on matters of cybercrimes. In April of the same year, a Commonwealth Cyber Declaration was agreed by the Commonwealth Heads of Governments to combat cyber crime and create new strategies for a good cybersecurity space. The INTERPOL had also held a conference in September relating to cybercrime to strengthen cooperation to prevent cybercrimes. In October, African countries had organized an African Forum on Cybercrime with cooperation of international organizations to fight cybercrimes. In November, the UN had adopted resolution which was title: *" Countering the Use of Information and Communication Technologies for Criminal Purposes".*

3.2 Legal framework on cyber attacks through international law system.

[93] European Judicial Training Network

3.2.1 United Nations and other international organizations on cyber attacks and operations.

The United Nation (UN) is an international organization that was founded in 1945 which is considered an important source of international law. The UN was established upon the Treaty of Versailles in 1919. its main headquarter is in New York City and it has other regional offices in Geneva, Vienna and Nairobi. According to the UN Charter, the aim of the organization is to maintain international peace and order in the international community. It also has other main important objectives like maintaining equal rights, self determination and achieving corporation between states as well as promoting human rights.[94]

The UN Charter is the main instrument of the organization, it contains all information needed to know how this legal body works. The charter discusses the organs of the UN, the membership, its purpose, the peaceful settlement of dispute, actions with respect to threats to the peace, breaches of the peace, and acts of aggression, etc. The UN is an important international legal body since it can make decisions that could be binding to states. Because the UN has the P5 powers that are committed to the organization, any decision that comes out of the General Assembly or Security Council could make the most powerful states from the P5 (China, France, Russia, the United Kingdom, and the United States) have a responsibility to maintain order and peace in respect of crimes that could lead to breach of peace including cybercrimes. [95]

The UN is considered an important legal body in international law and in matter of

[94] Mingst, K. , Fomerand, . Jacques and Lynch, . Cecelia M. (2022, July 27). United Nations. Encyclopedia Britannica. https://www.britannica.com/topic/United-Nations

[95] United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI, available at: https://www.refworld.org/docid/3ae6b3930.html

cyberspace, the UN is an example of state practice since it includes the presence of states as members of the UN and its an important part to the creation of new customary rules through comments and resolutions of the GA or SC. For example, the UN has an office that is responsible for crimes called : *"The United Nations Office on Drugs and Crime (UNODC)"* which is responsible for fighting against international crimes including drugs. It was established in 1997 and has 500 staff members. The UNODC works of straightening capacities to fight illegal international actions and prevent crimes that could possible breach peace. In 2002, the GA had given its approval on a program to fight terrorism. [96] The UNODC is considered an important legal resource for crimes related to cyberspace. The office has the capacity to fight cybercrimes by supporting the national structure and action of a state. It brings expertise in criminal justice system to provide technical assistance and preventing, building, raising awareness, bring international cooperation, data protection and cybercrime researches and analysis. [97]

The UNODC usually held *"Open-ended Intergovernmental Expert Group Meeting on Cybercrime"*. The first meeting was held from 17 to 21 January of 2011, the second meeting was in 2013 and the third was in 2017. In May 2017, the Commission on Crime Prevention and Criminal Justice made a request to the Expert Group to make keep doing meeting to discuss cybercrimes, the UN even came up with the resolution 65/230[98] and resolution 26/4 [99] . In 2013 the UN came up with a comprehensive study on cybercrimes which focuses on the impact of cybercrimes on an international level and the

[96] See more information about the UNODC at their official page: https://www.unov.org/unov/index.html

[97] UN, Office On Drugs and Cries. Cyber crimes. See mre at: https://www.unodc.org/unodc/en/cybercrime/index.html

[98] The UNGA adopted the resolution 65/230 which was based on the Salvador Declaration Article 42. The resolution made a proposal of an open-ended intergovernmental expert group to make a study of cybercrime. See more at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/526/34/PDF/N1052634.pdf?OpenElement

[99] Resolution 26/4 about Strengthening international cooperation to combat cybercrime. See more at: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_26/CCCPJ_Res_Dec/CCPCJ-RES-26-4.pdf

international cooperation in criminal matters. The study examined many problems of cybercrimes related to the government, the private sector, organizations and academies. The research study covered many topics including cybercrime legislation and framework. [100]

December 2019, the UNGA adopted a resolution in its report of the Third Committee (A/74/401)] 74/247 in relation to the use of information and communications technologies for criminal purposes. [101]The UNGA had introduce an Ad Hoc Committee to elaborate an international treaty on cybercrime. The treaty was first proposed by Russia which has gained a lot of support from the UN. However, the treaty is still under discussion even though it had gained many votes in favor since it is considered a bit dangerous for it's possibility to criminalize free expression and undermine privacy. [102] Russia's intention to create a UN Treaty for cybercrime is to replace the Budapest convention which is the first international convention called the cybercrime treaty created in 2001 by the Council of Europe. The convention itself is a criminal justice treaty that fights attacks against and by means of computer. By 2016, 50 states had joined the treaty including Israel and the U.S. Other 17 countries had signed it or been invented, and since Russia isn't a party to the convention, it wants to create its own international treaty with the help of the UN. [103]

Furthermore, the UN compromises with other UN Treaty that concerns

[100] UNDCO, 2013. Comprehensive Study on Cybercrime. See more at: https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf
[101] Resolution adopted by the General Assembly on 27 December 2019 [on the report of the Third Committee (A/74/401)] 74/247. Countering the use of information and communications technologies for criminal purposes. See more at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement
[102] UN, 2022. A UN treaty on cybercrime en route. See more at: https://unric.org/en/a-un-treaty-on-cybercrime-en-route/#:~:text=THE%20NEW%20TREATY,elaborate%20a%20comprehensive%20international%20convention.
[103] GFCE, 2016. The Budapest Convention on Cybercrime: a framework for capacity building. See more at:https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/#:~:text=The%20Budapest%20Convention%20is%20a,more%20effective%20and%20subject%20to

cybercrimes. For example, the United Nations Convention Against Transnational Organized Crime (2000) which is known for its second name the Palermo Convention, is an international treaty that treats international crimes. Although the treaty doesn't explicitly addresses cybercrime, it is quite relevant since it talks about any international crime. A cybercrime can happen at an international level which means that this treaty could address implicitly any cyber crime or attack. For instance, Article 2 (a) defines an organized criminal group as those of three or more persons which commit crimes in a period of time to gain financial and material gains in a way or another. The term organized criminal groups can also be intended to cyber criminal groups who gather to perform a cyber crime or operation to gain financial benefits which is the most commune objective of these groups. [104]

Another convention that could tell more about illegal crimes through cyberspace is pornography. The Convention on the Rights of the Child (1989), Article 34 of the Convention addresses the states to take obligation of child protection in any related matter to sexual exploitation and abuse including matters of pornography and prostitution.[105] Through cybercrimes many criminals try to use cyberspace to child pictures, videos or in real life to pornography activities. If a relative crime is committed by a state directly it could lead to a serious breach. Moreover, if cyber criminals that belong to a certain state have engaged in child pornography crime of another state this might be interpreted as a cyber warfare or cyber international crime which could make the state look responsibly of its civilian cyber criminals.

---

[104] UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME AND THE PROTOCOLS THERETO. (2004). UN Offie of Drugs and Crimes. https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

[105] See more at: https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/crc.pdf

The Council of Europe[106] also shares treaties that could relate to cybercrimes such as the Budapest Treaty mention earlier before, the Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems (2003) that criminalizes those who act illegally through internet and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007) which also prohibits the use of computers to access child pornography. The Council also tries to combat cyber crimes through other gateways like the Convention Monitoring Committee[107] which represent the state parties that are part of the Budapest Convention on cybercrime. According to Article 46 of the convention, the committee has the right to exchange information and consider any future amendments. Also, the council sponsors every years an annual cyber crime conference.

Other international organizations that could help dealing with cyber crimes is the International Criminal Police Organization (INTERPOL) which works to protect crimes of cyberspace. The International Telecommunications Union (ITU) is also a UN agency that helps harmonizing technical standards related to telecommunication and information. It partners with the UNODC and the UNICEF also. Other Non-Governmental Organizations include the Anti-Phishing Working Group (APWG) that combats cyber crimes like phishing and email spoofing. The Spamhaus which is responsible of tracking cyber threats and many other like the International Association

[106] The Council of Europe is an international organization that was stablished after the second world war. It is separated from the European Union because its membership extends further to other states, it is responsabiliy for human rights protection, democracy, the rule of law and uniform standars.

[107] Council of Europe. (n.d.). *Cybercrime Convention Committee*. Cybercrime. https://www.coe.int/en/web/cybercrime/tcy

of Internet Hotlines (INHOPE), the Internet Watch Foundation (IWF) and The Rand Corporation.

So by being said, after looking at all the committees and organizations within the UN, this can reflect some form of customary international law and an important legal body that can resolve legal matters in the context of cybercrimes. Even the UN had discussed several times on creating a new UN treaty for cybercrimes in 2019. The UN had worked on cyber crimes matters since the 2010s and in 2012, the UN had initiated a study in its GA Resolution 65/230 which conducted a study organized by the UNODC in Vienna entitled, *«with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime»*. All of these initiatives by the UN and their expert groups include the two main important elements of the customary international law which is Opinio Juris where experts in international discuss and try to come up with solutions and new suggested custom rules and resolutions from GA and SC that involves the presence of a state practice. All of these elements discussed above show how the United Nation system and other organization can work to combat cyber attacks and prevent them from escalating into a war between states, which shows how of an importance is the UN system in implementing order withing the international society when dealing with cyber attacks.

3.2.1 Article 2(4) of UN Charter and Article 49 Protocol 1 of Geneva conventions.

The UN Charter is an important legal source when it comes to decisions and prohibitions about specific matters. Article 2(4) consists an important point regarding cyber attacks as a way of using force. This specific Article states that all members

should not use threat or force against any territorial integrity or political independence of a state in their international relation matters. This article is a good start to as relate if cyber attacks can be considered a type of force which is a topic that will be discussed and analyzed more in the next chapter of this thesis. Meanwhile, it is important to discuss the fact that military attacks are prohibited by this article except when there is a case of self defense or by an authorization of the SC[108].

However, one problem arises in relation with the concept of force in the UN Charter is that the charter itself has never defined the word "force" which can be interpreted in different ways. Since the charter was entered into force after the Second World War, force itself can be understood as the tools that were used in that era while military attacks happened, such as tanks, planes, nuclear weapons and other arms. But, looking at the technological development in the 21st century, force can be seen from other perspective which can be interpreted as the use of any tools that consists of power and could lead to an attack.

Article 51 also discussed the fact that the charted wouldn't impose states or individuals to self defense if an armed attack occurs. This specific article could create a dilemma of debates surrounding the term force, because states would debate the fact that only kinetic weapons are prohibited to use in any kind of situations, by that means if we want to considered the cyber weapons and the different tools of wars that has been developed, these weapons could be used legally in cases of self defense.[109] Moreover,

[108] Waxman, M. C. (n.d.). Cyber Attacks as "Force" Under UN Charter Article 2(4). Scholarship Archive. https://scholarship.law.columbia.edu/faculty_scholarship/847/

[109] (PDF) Article 2(4) and Cyber Warfare: How do Old Rules Control the Brave New World?. Available from: https://www.researchgate.net/publication/314502083_Article_24_and_Cyber_Warfare_How_do_Old_Rules_Control_the_Brave_New_World [accessed Aug 24 2022].

many specialist have discussed the reality of cyber warfare and attacks and how they violate the UN Charter Article 2(4), assuming that its prohibited the use of force no matter what situations is and the fact that cyber weapons constitutes of power and a way of using force illegally.

Another point to note is the fact that cyber attacks could also be considered an armed attack and could possible violate International Humanitarian Law if it violates Article 49 Protocol 1 of Geneva Conventions which defines the word " Attacks" as an act of violence against an opponent whether in situations of defence or in offence. The concept attack under IHL does not mention anything specific related to the type of attack, the weapons used in attack, the nature of the attack itself or any matter related to an attack which means that any aggression, force, crime could be defined as an attack including cyber ones.

Chapter 4: International law and cyber attacks.

International Law is the law that governs states and their relations in the international arena. It also governs the relation between states and organizations. International law is considered almost binding to all states and it became a legal source that states seek it when there is an international issue. International law is considered a legal body that tries to bring stability and security between states by creating rules for state to try to follow. However, its only issue is that sometime it is not binding to states.

International law is part of the international relation domain even though there is difference. States usually respect international norms and rules and try to be careful with their actions because if they act otherwise the state could be regarded negatively from

the international community. The international law system is not enforced by military means or economic sanctions but rather by reciprocity and self interest sense. If a state breaches an international norm it could be judged in future relations with other states. If continuous breaches occur the value of the international system would be reduced and there wont be order, which is why states are somehow compelled to the rules.

Since IL has a major interest in states, its principles also governs the relations between them in different fields. The major source of IL is the UN Charter which explains the main principles of IL including human rights promotion, state sovereignty and the use of force under IL. It is important to apply these principles to cyberspace and explain each of them in regards of cybercrimes and cyber attacks. This chapter will mainly focus on international law topics and how are they explained and applied in terms of cyberspace, cyber attacks and cyber crimes. This topics include, sovereignty, non-intervention, self defense, due diligence, neutrality and international responsibility. The chapter is important to answer our key questions and analyse our perspective regarding this matter.

4.1 The principle of sovereignty and cross border cyber attacks.

The principle of sovereignty is one of the most important principles under IL. To choose to talk about it first is very important since cyber attacks are to be considered illegal and unlawful if it breaches the most important principle in IL,and since the thesis focuses on cross border cyber attacks , then it would be essential to talk about sovereignty since it is the principle which studies the structure of the international legal order. It is one of the most fundamental principle to understand ones state relation between its statehood and territorial space. The concept of sovereignty itself involves

topics regarding territorial jurisdiction, immunity and the principle of non-intervention. The UN Charter Article 2(1) follows up that states have a supreme authority over their territories, an immunity over other states own jurisdiction and their freedom of others states intervention.

The concept of sovereignty have been argued among many specialist. Some think that the concept have a supranational and political meaning and others see it as a new form of a political authority such as the EU for instance. The term itself has been discussed among theorist like Hobbes which has linked the term sovereignty with his social contact theory which explains that the supreme authority of a state should let the people escape from civil wars through a fictive social contact. On the other hand, John Locke had also explained the fact that states cannot get their supreme authority from a social contact among people but rather from a contact between the people and the state which means that for him sovereignty is limited and its bind by a legal source[110]. Other theorist like Grotius, Gentili and Suarez have defended the idea that sovereignty is linked to disciplinary interventions and limitation. [111]

Jeremy Benthams had also found the idea of a limited sovereignty[112] and Rousseau had explained how states exercise sovereignty of political institutions for the respect of a general will.[113] He had differentiate the concept of popular sovereignty and political sovereignty arguing that if a state does not respect the people's will, it has risk of losing

[110] Singh, R. (1959). JOHN LOCKE AND THE IDEA OF SOVEREIGNTY. The Indian Journal of Political Science, 20(4), 320–334. http://www.jstor.org/stable/42743527

[111] Somos, M., & Smeltzer, J. (2020). Vitoria, Suárez, and Grotius: James Brown Scott's Enduring Revival, *Grotiana*, *41*(1), 137-162. doi: https://doi.org/10.1163/18760759-04101007

[112] Hart, H. L. A. (1967). BENTHAM ON SOVEREIGNTY. Irish Jurist (1966-), 2(2), 327–335. http://www.jstor.org/stable/44026042

[113] Canon, J. (2022). Three General Wills in Rousseau. The Review of Politics, 84(3), 350-371. doi:10.1017/S0034670522000328

its attribution. Other concepts and links around years have been followed up with the idea that there is a link between popular sovereignty and democracy where people ruling a body of law is the subject of sovereignty. [114]Which is why the concept sovereignty was linked to IL, meaning that if a state wanted to have its internal sovereignty protected it had to be submitted to public international law. However, to do that states had to have consent of mutual rights and obligations.

IL was developed after the Vienna Congress in 1815[115] which began to coexist between sovereign states. It had covered everything from external sovereignty, internal sovereignty, border regulations and dispute settlements. It had protected states from the intervention of other states which gave states some sort of immunity. When IO where created through which states former their external affairs the relationship with the IL system became even more efficient. Since modern IL was developed, the concept of sovereignty was also internationalized to modern sovereignty. With the emerge of international cooperation , the concept external sovereignty was more clear, specially when it was notice in the Lotus case with the ICJ where sovereignty was conceived as limited and law-based. According to the court in its 1923 Wimbledon case, the right to enter into international engagement is an attribute itself of state sovereignty. [116]

Since IL deals and cares of a state sovereignty, it is to note that domestic law is also a part of an internal sovereignty. The concept of sovereignty has been also linked to internal affairs and external affairs too. The difference between these two concepts

[114] Yack, B. (2001). Popular Sovereignty and Nationalism. Political Theory, 29(4), 517–536. http://www.jstor.org/stable/3072522

[115] The Congress of Vienna of 1814–1815 was a series of international diplomatic meetings to discuss and agree upon a possible new layout of the European political and constitutional order after the downfall of the French Emperor Napoleon Bonaparte.

[116] Hyde, C. C. (1930). The Interpretation of Treaties by the Permanent Court of International Justice. The American Journal of International Law, 24(1), 1–19. https://doi.org/10.2307/2189296

should not be conflated between domestic and international sovereignty. International sovereignty regulate the legal order of a state. Domestic sovereignty regulates both internal and external affairs of a state. The absolute sovereignty, another concept with has been emerged, meaning that sovereignty can be inherited from domestic law. On the contrast, limited sovereignty can also be presented as ultimate and final meaning that it is inherently limited. It is known that the concept of sovereignty implies a certain degree of intensity which requires competences being said, sovereignty sometimes has to limited.

Finally, the concept of unitary and divided sovereignty had also appeared which analyses the divisibility of sovereignty. A unitary sovereignty implies a system where national governments are sovereign which explains the fact that a state can be divided into provinces, counties but they are also considered administrative subdivisions. In the case of divided sovereignty, the state is limited on its authority based on *jus cogens* norms which prohibits violations of basic human rights.

Since IL is based on the presence of states, it is important to admit that a states sovereignty is an important subject under IL, meaning that each state has the freedom to determine whether they want to enter into a relation with other state or not. A state usually qualifies as a respectful state if it's sovereignty doesn't stand alone which means that a state territory should be in connection with a population. An important element of a state's sovereignty is to have an equal sovereign status as it is mentioned in the UN Charter and in the GA Resolution on Friendly Relations (2625-1970)2 (FR Resolution) [117]and in the CSCE Helsinki Final Act (HFA) of 1975[118]. According to the FR

[117] United Nations General Assembly: Resolution 2625 (XXV) Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation Among States in Accordance with the Charter of the United

Resolution any state should have sovereign equality meaning that it has equal rights and duties and all members are equal under an international community regardless of the economic, social and political differences. [119]

A sovereign equality of a state enhances that a state should have its territorial integrity and political independence equal of any state, it encompasses the right for any state to have also juridical equality as well as the right to choose how its political, economic and cultural system is defined. Since a state has an extreme authority and power due to its sovereignty, it is fair to say that states have the right to belong to any IO, to be part of any bilateral or multilateral treaty, to be party of a treaty alliance and even the right to neutrality. Because a state sovereignty is connected with a territorial and population of a state, it has to respect the sovereign status of another foreign state, as well as its own state. By this said, a state sovereignty is limited as its stated in the two UN 1996 Covenants (Covenant on Civil and Political Rights[120] and Covenant on Economic, Social and Cultural Rights[121]).

Under the UN Charter, Article 2 (4): a state should not use force against another state territorial integrity or political independence. Since sovereignty means

---

Nations. (1971). The American Journal of International Law, 65(1), 243–251. https://doi.org/10.2307/2199350

[118] Organization for Security and Co-operation in Europe. (1975). Final Act of the Conference on Security and Co-operation in Europe. Organization for Security and Co-operation in Europe. See more at: https://www.osce.org/files/f/documents/5/c/39501.pdf

[119] Roth, Brad R.2011, 'The International Law of Sovereign Equality' *Sovereign Equality and Moral Disagreement,* online edn, Oxford Academic, 19 Jan. 2012), https://doi.org/10.1093/acprof:oso/9780195342666.003.0003

[120] International Covenant on Civil and Political Rights; ADOPTED 16 December 1966 BY General Assembly resolution 2200A (XXI). See more at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[121] International Covenant on Economic, Social and Cultural Rights; ADOPTED 16 December 1966 BY General Assembly resolution 2200A (XXI). See more at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights

independence when dealing with relations between state, meaning that a state is not subject to a higher authority. A recognition of a state sovereignty means to create a basis for it under an international legal system.[122] And because sovereignty is associated with power and legitimacy as the freedom to have independence and the non interference with other external power for foreign states, it's quite interesting to see how the principle of sovereignty is applied to cyberspace and if cyber attacks could violate a states sovereignty in any form.

Cyber operations are increasing nowadays between states. An estimation has been detected that over 22 states conduct cyber operations that targets other states and these operations are growing more. The thing about using cyber operations in practice is that they do not necessarily cause physical effects even though they are used as a way of force. According to the UN Charter if a cyber operation causes injury or death to persons then it could be described as an armed attacks and a way of using force. For example, the NotPetya attacks which was a malware attacks on companies and governments of Europe-wide. The attacks was attributed to Russia by a large number of states in 2018. Also, another attacks in 2018 which targeted universities was attributed to Iran by the U.S and the UK. At the same year, Russia was attributed an attack by the U.S and the UK which consisted of an attack at specific router to promote espionage and theft of intellectual property. In December of the exact same year, China was also attacked by a group of espionage. It's to be stated that China had suffered a lot of economic loss because of ransomware attacks.[123]

---

[122] Zainab, N., Agung Noviardi, D., & Eka Buana ZK, F. (2018). Violation on State Sovereignty by Military and Paramilitary Activities on Nicaragua vs United States Case. SHS Web of Conferences 54, 05001 (2018). https://www.shs-conferences.org/articles/shsconf/pdf/2018/15/shsconf_icolgas2018_05001.pdf

[123] Ransomware attacks are types of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the

In the past, states weren't being able to attribute cyberattacks, it was very challenging and difficult because attackers operate in a specific speed from different servers which makes it difficult to detect and expose their identities. However, technology has improved and has a greater ability to attribute cyber attacks specially when dealing with private cybersecurity companies. Nowadays, states tend to attribute cyberattacks to other states and many states work together to attribute cyber operations. Which leads us to the discussion that states have agreed that IL applies to cyberspace including the principle of sovereignty and non-intervention in spite of the lack of legal force on cyber activities by IL.

Since new phenomenons appears every day, the fact that cyber attacks is not applied by IL is a wrongful said because the paradigms of IL also develops according to the development of events that is caused by the international system. In 2013 and 2015 in an UN GGE, states had agreed that IL is applicable to cyberspace activities. It was mentioned that a state sovereignty principle is applicable to a state conduct of ICT related activities and also to their jurisdiction over ICT infrastructure within the territory of the state.[124] Further, experts had agreed that if a state uses ICT they have to observe and focus on state sovereignty and sovereign equality of another states internal affairs.

The principle of sovereignty focuses on the supreme power of the state as in an authority and protects the territorial integrity of a state. One of a states sovereignty principle is the prohibition of intervention into other states affair and any behavior that

---

ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever or the ransom increases. Under international law ransomware attacks are considered illegal since they are cosidered a national security problem that threates the security of a state and is considered an illegal act that shows signs of economy stealing and war creation signs.

[124] A contribution that was submitted by the United Kingdom's Multi-stakeholder Advisory Group on Cyber Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015. See more at: https://www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf

consists coercive means which could harm another state. There are two schools that discusses cyber activities within sovereignty context. One discusses the non intervention principle which will be discussed latter on which applies to certain cyber activities and that an unfriendly behavior from a state could breach international norms which affects a states responsibility. On this view, it is to understand that IL guides a state interaction however it does not rule it as a primary rule when it comes to cyber matters.

The second school discusses the fact that cyber activities can be unlawful acts which constitutes a violation of a state sovereignty as it is mentioned in the Tallinn Manual 2.0. However, states and IO have been not been active and even silenced when it comes to cyber debate and the question of sovereignty. For example, Estonia had addressed some aspects of how IL could be applied to cyberspace but, it has not address the issue of sovereignty or non-intervention. Iran had stated that the use of illegal activities by the ICT could result in a breach of a state sovereignty and internal affairs but without expressing how IL applies in practice. China had also addressed in 2017 by its International Strategy for Co-operation in Cyberspace that sovereignty applies in cyberspace and that not a single state should interfere into others affair using cyber activities that could result into a harm in its national security.

In 2019, the Netherlands government had also stated that cyber operations violates a state sovereignty and every internal and external aspect of sovereignty applies in a cyber domain.[125] At the same year, France had also given its view regarding cyber means explaining that any unlawful cyber operation that could violate the French system constitutes a violation of the French territories which causes a violation of its

[125] Tsagourias, N. (2021, December 14). Chapter 1: The Legal Status of Cyberspace: Sovereignty Redux? Elgar Online: The online content platform for Edward Elgar Publishing. Retrieved February 6, 2023, from https://www.elgaronline.com/display/edcoll/9781789904246/9781789904246.00010.xml

sovereignty. Since there is not a single opinio juris that marks any opinion on whether sovereignty principle is applicable to cyber activities, then customary international law and existing principle are applicable to a state activities in cyberspace.

When arguing whether cyber activities violate a state sovereignty, its important to considered the three elements of sovereignty. Within this claim, it's important to consider a state's land territorial and boundaries, its aerial space, territorial sea and maritime zones. The law on the prohibition of use of force as well as customary law can reflect how cyber activities breaches a territorial integrity of a state. Furthermore, the principle of sovereignty includes the right of a state ho exercise jurisdiction within its territory, by that means jurisdiction can be either have the power of prescription, enforcement or adjudication. Also, a state should respect by any time and means the independence and authority of other states.

Moreover, a state should not exercise its authority in another territory and this includes the rule of use of force which is dictated in the UN Charter and customary international law and principle of non-intervention in internal affairs of another state as well as the law of sea and air as its incorporated in the UN Convention on the Law of the Sea[126] and the Convention on International Civil Aviation (Chicago Convention)[127], as well as Status of Forces Agreements[128] and the Vienna Conventions on Diplomatic Relations and on Consular Relations.[129]

---

[126] Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397

[127] International Civil Aviation Organization (ICAO), Convention on Civil Aviation ("Chicago Convention"), 7 December 1944, (1994) 15 U.N.T.S. 295, available at: https://www.refworld.org/docid/3ddca0dd4.html

[128] United Nations Protection Force (UNPROFOR) - Status of Forces Agreement (SOFA); Date(s) 1992-04-15 - 1993-01-05. Found at: https://repository.usfca.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1218&context=usflawreview#:~:text=Claude%2C%20Status%20of%20Forces%20Agreements,21%2D22%20(1987).

[129] Vienna Convention on Consular Relations 1963. See more at: https://legal.un.org/ilc/texts/instruments/english/conventions/9_2_1963.pdf

The debates starts to be considered when it involves around whether the notion of sovereignty applies to cyberspace or not. It is to be noted that a violation of a territorial integrity includes physical incursion into another state territory either by land, sea or air. But since cyber activities have a tangible and physical aspect because of the use of computers, the interaction is considered virtual because the transmission of data and the content that is being exposed or targeted is done through physical devices which could be difficult to analyse how it violates a territorial boundary. It is to be noted, that since a cyber infrastructure is located in a particular area then a cyber activity is being detected from a specific territory which means that the state could be responsible. However, because cyberspace is often not territorial then the geographical border is difficult to detect.

What's interesting to discuss is that cyberspace is not managed alone by itself. its existence involves real people in a territorial space and its equipment which is located also from a specific territory is managed by a government or a company, which means that any engaging activity that involves malicious acts could result in causing an effect to another territorial jurisdiction, and since a state exercises its sovereignty over cyber infrastructure, over persons within its territorial boarder, therefore the principle of sovereignty applies to cyber activities. By this means, some states have law regulations to manage cyber activity in their territory like laws processing data and content on internet, as well as approaches to limit peoples behavior to respect sovereignty and not intervene into any internal affair.

An important matter to discuss is when does a state violate the sovereignty of another states. A state breaches a territorial integrity of a state when it exercises actions

related to that state without its consent, for example Nicaragua had violated the territorial integrity of Costa Rica by exercising certain actions on its territory without its consent just like the ICJ stated[130]. Another example can be set in the Corfu Channel case when the ICJ stated that the UK had violated the territorial integrity of Albani by routing warships and conducting illegal operation it the other country's water without its consent, this had constituted a breach of sovereignty and an intervention with the use of force which resulted in legal consequences. [131]

In a case where the violation of a sovereignty is done remotely, meaning that a state can violate another states sovereignty without causing physical damages in the affected territory. For instance, in Switzerland, some FBI agents had interrogated bankers by telephone without the consent of Switzerland and they forced them to complete a questionnaire under the use of threat to be under subpoena if they do not cooperate, this had resulted in violation of Switzerland territory and sovereignty[132]. In case of cyber context, scholars had conclude in Rule 4 of the Tallinn Manual 2.0 that a State must not conduct cyber operations that could violate a state's sovereignty. For example, if a state had managed to do a cyber intrusion into another state cyber infrastructure with the exercise of a states power this in some way could constitute a violation of sovereignty similarly as in the case where a state shuts down another states power grid on the latter state's territory.

So when a state tries to do an international wrongful act or violate the sovereignty

[130] ICJ, Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v. Nicaragua). 2015. See more details at: https://www.icj-cij.org/public/files/case-related/152/18846.pdf
[131] Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania). 1946. See more details at: https://www.icj-cij.org/en/case/1
[132] Moynihan Associate Fellow, H. (2020, October 1). 2. the application of sovereigntyin cyberspace. Chatham House – International Affairs Think Tank. Retrieved February 6, 2023, from https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace

of a state by targeting a state cyber infrastructure, or spy on a state to gather information, or exposing the latter with its weaknesses within the system and plan a future attack, this can lead to a violation of territorial integrity. However, proving the act of violation of sovereignty by cyber means is complicated by the fact that states have different views of how it constitutes a violation. So, even if the approach is considered accepted, the analysis is challenging since there is not many attributes to cyberspace. Just like Netherlands had argued, a cyber attacks cannot be made up from several actions by several countries, it is often made simultaneously and it cannot be traced which makes it difficult to determine if the cyber operation had a cross-border element that violated the sovereignty of a specific state[133].

To conclude, sovereignty is an essential rule of IL and a state should not conduct cyber operations that could breach a state's sovereignty. If a state causes physical damage or cyber infrastructure lose can be taken into consideration as a violation specially if the violation resulted in interfere with data or service that is necessary for the exercise of governmental functions as well as civilians private life. If the malicious act constitutes of an interfere in citizen, social services, the conduct of election, collection of taxes, performance of national defense activities or manipulation of police communication it is considered a violation of a state sovereignty if the act was conducted from another territory of another state. Brief, the degree of violation of a sovereignty depend on the case of a cyber operation.

---

[133] Schmitt, M. (2021, April 19). *The Netherlands releases a tour de force on International Law in Cyberspace*. Just Security. Retrieved February 6, 2023, from https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/

4.2 Due diligence

Due diligence is an important topic in international law. It is defined as the degree of care that states reach in a reasonable way and legally required. The concept was related to mediate inter-state relations and now as the state's neutrality and the protection of aliens. The concept of due diligence refers to the obligation that a state has by not allowing its territory to be used for acts that are contrary to the rights of other states. [134] it is also essential to note that the due diligence principle can entitle a state to be responsible for individuals acts and also responsible in case where it fails to take measures to prevent the effects made by private persons. In the Corfu Channel judgment, the ICJ emphasized that every state is under the obligation to not allow by full intention to allow its territory to be used for contrary actions to the rights of other states.

In the case where cyber activities occur, the due diligence requires states to take actions and measures against these operations in certain circumstances.[135] First, when a cyber act is conducted by a non-state actor or a third state from a territory where the cyber infrastructure is under its control in the territory of another state, the state where these non state actors have committed the cyber operation, the state is considered responsible for its actions regardless whether they were operating under the authorization of the responsible state or not, and the reason of that is because a state should always take measures against these incidents, an attack to a country is an attack to its civilians, territory and sovereignty. An individual who acts alone should know that operating a cyber activity can result in harming civilians and causing damages to civilian objects, in this case it would potentially lead to a cyber war and the responsible

[134] Mundi, J. (n.d.-a). Wiki Note: Due Diligence. https://jusmundi.com/en/document/publication/en-due-diligence-1

[135] International cyber law: interactive toolkit. (2022a, September 12). Due diligence. International Cyber Law: Interactive Toolkit. https://cyberlaw.ccdcoe.org/wiki/Due_diligence

state would know whats happening, so the state takes responsibility of the action specially in case where it has actual knowledge of these acts.

To clear the idea, if a state hasn't any knowledge on a wrongful cyber act happening on its territory, it should include measures and capacities to detect and stop such acts. Even if a state has limited technical capacities which would make it look weak and fail to detect a malicious ICT act it should seek political and diplomatic measures including counter-measures or refer to the UNSC. A state that does not take all the reasonable measures needed to detect a cyber wrongful act and is incapable to detect them cannot have an exception to the prohibition of the use of force. In other sayings, the state should always be expected to respond to third party actors in cases where cyber acts are happening withing its territory.

4.3 The context of cyber attacks in international humanitarian law.

International Humanitarian Law also now as the law of war (IHL) is the law that sets rules that has humanitarian purposes which tries to limits the effect of an armed conflict. IHL protect those who are considered civilians, meaning that they do not are participating in a hostility. The law itself restricts the means and methods of warfare. This specific law governs the relation between states in humanitarian matters, by agreements between them which involves treaties and conventions which are legally binding. The IHL does not limit a state to use force but rather limits the consequences from using force by a state.

IHL is derived from the four Geneva Conventions of 1949 and the La Hague Conventions of 1899 and 1907 which are the main sources of international humanitarian

law and most of the states are bind by it since they have agreed to be part of the convention. The four Geneva Conventions have been developed to the Additional Protocols of 1977 which concerns the protection of victims in an armed conflict. Further, the convention sets rules for how to use specific weapons and which are prohibited including military tactics. The la Hague conventions were adopted to regulate warfare, it had first included both international peace conferences in 1890 and 1907 and the 1954 Hague Convention on the Protection of Cultural Property in the event of armed conflict. It governs the means and methods of warfare and conduct of hostilities to protect war crimes.

Other agreements that are related to the same matter include the 1972 Biological Weapons Convention; the 1980 Conventional Weapons Convention and its five protocols; the 1993 Chemical Weapons Convention; the 1997 Ottawa Convention on anti-personnel mines; the 2000 Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict.

It is important to note that IHL only applies during an armed conflict and it ends when the war is done, and it applies equally to every side regardless who is the attacker and who is the targeted one. It also applies to international armed conflicts and not non-international armed conflicts unless the national conflict is so violent that rises to be an international one. It is also important to note that IHL is a bit different from International Human Rights Law (IHRL) since they have different treaties that governs them. The HRL applies in peacetime while IHL is only applied during the armed conflict once it is begun. The IHL covers the areas of protecting those are not part of a hostility and those who are no longer taking part of it from civilians to medical and

religious military personnel. It also protects those who are injured during the conflict such as wounded, shipwrecked, sick combatant and prisoners of war. [136]

When discussing about cyber attacks and IHL or HRL it is important to study the elements that are found in cyber operations or attacks to observe whether they breach IHL or not? The concern arises by the fact that cyber operations are becoming part of military operations and they are used as a way to cause an armed conflict. A cyber attack can happen at the worsts situations like when a system is already vulnerable and unprotected, this can lead to devastating consequences and put civilians in a more dangerous situation. Nowadays, we see that technology is also being a major part in supporting humanitarian programs which means that the technology era had made the two way communication between civilians and humanitarian staff more easily which makes the gathering of information faster. However, because of the development of cyber attacks and vulnerabilities that technology can face, cyber operations could impact a persons life from its own home and making humanitarian emergencies in danger. [137]

Lets take a hypothetical example from our own. If we want to consider that cyber attacks can harm a population by using malicious technology, it can cause harm and danger like misuse of information, disinformation, hateful speeches and even propaganda. This could risk a civilian life to reach a certain physiological level where he/she would feel unable of continuing anymore, this could constant a breach of IHRL. Another example, is how cyber attacks can also breach IHL not also IHRL. If a cyber

[136] Rezek, Jose-Francisco. “Wounded, Sick and Shipwrecked Persons.” In International Dimensions of Humanitarian Law , 153–66. Geneva: Henri Dupont Institute, 1988.
[137] Ramluckan, T. (2020). International Humanitarian Law and its Applicability to the South African Cyber Environment. Journal of Information Warfare, 19(3), 102–117. https://www.jstor.org/stable/27033635

attack was made in an active war using cyber means to support military activities could make an armed conflict even worse than a normal one which means that cyber attacks not only can violate and affect an individual as a human rights case but also civilians who are placed in a position where they face war and they are not involved with it which can be affected by these cyber attacks specially if the attack had rose it to even a worse one.

Arguments have been discusses regarding cyber attacks when applying IHL or IHRL and of these is when dealing with computer systems. IHL protects civilians from any danger in an armed conflict whether its from a cyber attack or not, but it does not protect the computers, medical devices and networks in a case of cyber attack. According to the ICJ, IHL applies to cyber operations and it limits its activities during an armed conflict just like it limits the use of any other weapon.

Other arguments related to IHL and cyberspace is whether civilian data is considered as a civilian object. Many experts have disagree to this by interpreting that it is not the same, but if we try to analyse the nature of a civilian object is anything that is not considered a military object. If we look a civilian data as a shield or an object that is consider super important which contains important information that would harm economically or physiologically a civilian in case of destroyer or a leak then it would be adequate to say that a civilian data is considered a civilian object specially if it was destroyed in a place where an armed conflict happened.

Furthermore, the fact that IHL applies to cyber attacks does not mean that it legitimize cyber operations during an armed conflict, since it does not legitimize any other form of warfare. In fact, the idea of legitimatizing cyber warfare is becoming a

fear between states. In a case where cyber attacks can become legitimate that's when the international order would become aggressive and unstable because cyber attacks are just like any other traditional attack and sometimes its even worse. The idea of legitimatizing cyber warfare can create an international war between states and it would cause first a global economic loss which can lead to hunger if its not controllable as well as a humanitarian crises if cyber attacks where to be attacked towards hospitals and medical staff. Cyber attacks must be a major interest in the future and bringing new articles and rules related to cyber operations in IHL must be a discussion to make.

4.3.1 The use of cyber means in military activity: Military aims and objects under IHL.

As discussed above, we have reached the conclusion that cyber attacks violates not only international humanitarian law but also international human rights law. But, is also important to discuss profoundly how cyber attacks are being managed under IHL in the context of military aims and objectives since cyber attacks are not only used in peace time but also in war time. Rule 8 of IHL states that military objectives are those that make an effective attribution to the military action considering their nature, location and purpose of use.[138] They have the aim to make destruction, capture or neutralization which is a military advantage. The definition of military objectives is also defined in the Article 52(2) of Additional Protocol I of the Geneva Conventions.[139] Military objectives are considered legal and their use have an advantage to the military action and even

---

[138] International Humanitarian Law Databases; Practice relating to Rule 8.Definition of Military Objectives. See website: https://ihl-databases.icrc.org/en/customary-ihl/v2/rule8

[139] Article 52 - General protection of civilian objects. Visit: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-52?activeTab=undefined

when there is the presence of civilians some manuals have stated that such objectives does not render immune from attack even if they are not combatants.

Military objectives often include establishments, buildings , materiel and armaments, military means of transportation and communication, even economic targets that effectively support military operations are also an example of military objectives. In the advent of cyber means and objects, computers and technological weapons are also considered as pat of military objects. Cyber weapons in a military action can cause vulnerabilities in the infrastructure system such as attacking the energy, transportation and communication sector which can lead to a mission success for the attacker state. Aiming at the infrastructure systems of a state can lead to a critical situation since they support the conduct of military operations which is why many experts have been discussed the fact that cyberspace will be commonly accepted as a military domain of conflict.

One of the main reason of why states are now leaning towards cyber weapons more in military actions instead of kinetic weapons is because of the low cost of computing devices. Since computers are easier to use, attackers do not require a high sophisticated weapon to conduct a military attack, instead they use their computers and brains by building highly developed platforms like stealth fighters or aircraft carriers. For example, in 2009 Iraqi insurgents had used software for a low cost of 26$ which targeted the video imagery relayed by a US drone aircraft,which allowed them to see what the US military was seeing which is considered as a form of cyber espionage. [140]Secondly,cyber objects are highly advantage to the military aim and have a high speed. Cyber attacks usually are sophisticated and complicated to make because it

[140] MacAskill, E. (2009, December 17). US drones hacked by Iraqi insurgents. TheGuardian. Retrieved February 6, 2023, from https://www.theguardian.com/world/2009/dec/17/skygrabber-american-drones-hacked

contains millions of codes to make.however, if the attacker finds a single vulnerability, is enough to destabilize the situation and make the defender contend with the sophisticated codes.opposed to a conventional warfare, cyber operations in military action do not need hours to carry out with missiles and fire arms, its enough to take a whole nation within just minutes of applying the code.

Thirdly, which is a very important advantages of why states are now involving more cyber weapons in military actions is that they are difficult to detect and attribute.Since attackers cannot be seen nor they can detect their location an individual that works for the state can conduct a cyber attack from another country without necessarily being in the time of military action.cyber weapons have the advantage of well covering digital footprints which are difficult to detect.Also, an attacker can prepare a cyber attacks in a less visible way.

Using cyber means in military activity as an advantage to the military aim mission since they have software programming codes that could cause malfunction to any state infrastructure system. Computers are considered as military objects just like any other objects since their nature and localization can cause destruction and harm. Cyber weapons in military action can cause massive physical damage and economic disruption. Since the military strength comes from the economic vitality, so a state that does not have the strength to create highly developed cyber weapons can endanger the military mission aim and allow military vulnerability to expose which is why states need to acquire cyber security both in peace and war time. If the cyber security of a state is vulnerable, then this would have impacts on the military since it will allow to expose military cyber systems vulnerability and could result in damages.

4.3.2The use of force under cyber context

The use of force is an important notion in IL which concerns the relations between states which is related to the international use of force against another state or civilians of another state. In international law the use of force is regulated by treaties and it's used in the context of human rights when there is danger and threat to the international peace and security when dealing with human rights issues. The notion of prohibition to use force came into presence after world war 2 and specially after the technological development which led to the creation of nuclear weapons, biological and chemical ones which have devastating effects. The prohibition of the use of force became a rule that prevents war and it's notion can be quite complex in the international legal framework. Nowadays, the notion is secured by collective measures means and peaceful settlement of dispute means. Hence, since the Westphalia Peace Treaty of 1648, the international system had to enhance a new concept called international security which makes sure that no state intervenes into another states internal affair and cause a major threat to its security. [141]

The UN Charter had regulated the use of force in IL by maintaining international peace and security as states in it's Article 1(1) which includes the prohibition of use of force resulted of action of aggression, breaches of peace and any threat to peace. Under IL the use of force is prohibited regardless of the circumstances and cases. There has been many cases where the ICJ had found violation and breaches of peace by using force like the *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v The United States of America*) in 1986 and the *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* in 2005. Furthermore, the UN

[141] Heselhaus, S. (2014). INTERNATIONAL LAW AND THE USE OF FORCE. Encyclopedia of Life Support Systems (EOLSS). https://www.eolss.net/sample-chapters/c14/E1-36-01-02.pdf

provides that all its members should not use force of threat by force in their international relations and they can not violate the territorial integrity or political independence of any state. (Article 2(4) UN Charter).

However, the use of force can be consider legal if the act was authorized by the UNSC as part of a collective security mechanism and in act of self-defense. The UNSC can decide and determine the existence of any threat to peace by making recommendations and measures in accordance with Articles 41 and 42' (Article 39 UN Charter).

In cyber context, it is not easy to determine if a cyber attacks may constitute an element of use of force or threat. Many relevant treaties have mentioned some statements about the matter. For example, the North Atlantic Treaty Article 4 provides that all state parties should consult each other if any of their territorial integrity or political independence is threatened. The North Atlantic Treaty Article 5 states that if an armed attack is occurred to any of a European or North America state its considered an attack against all, and under Article 51 of the UN Charter they can attack including the right to use armed force as a matter of self defense to maintain the security within the space. Also, the United Nations Charter Article 51 gives the right to states for self defense if an attack was occurred against a UN member in order to maintain international peace and order.

For instance, the U.S Doctrine of 2012 had mentioned the question of whether cyber activities constitute a use of force under Article 2(4) of the UN Charter. According to Harold Koh the states legal advisor, a cyber activity can cause damages with result in death, injury and significant destruction because it is done by using a

method or a way of force. A cyber attack can meltdown a nuclear plant, it can cause flood damage by opening a dam, it can even make planes crashes and cause traffic air control. By being said, if the focus is on the ends rather than the means then a cyber attacks is qualified as a war under IL. Using a cyber weapon can produce a large effect which rises the level of use of force.

It is important to note that a cyber activity can rise to an act of armed attack which may trigger a nation to attacks under the right of self defence as stated under Article 51 of the U.N Charter. Further, under IL and its legal conventions like the Geneva and Hague Conventions and the UN Charter apply to cyberattacks without having an specific rule on its applicability. However, because of the difficulty of attribution resulted from the use of remote computers and the possibility for a third country harm from a cyberattack, it is difficult to apply legal conventions. The law would be clearly applicable in case of clear physical damage. [142]

The application of use of force is indicated also in the Hague Conventions and the use of armed forces as a military necessity, in case of human rights, chivalry and proportionality. However, if a state is conduction cyber operations is case of military means it can trigger a cyber war which can escalate to be considered an armed war. By that, the UN Norm A 2004 UNGA resolution called for a convening of a report by a group of government experts (GGE) from 15 nations included the U.S to make rules and regulations to secure cyberspace. The GGE included rules like not damaging a states infrastructure with cyberattacks by intentional means and not targeting a state cyber emergency responds. Further, the UN Resolution 70/237 states that members should

[142] Valuch, J. (2020, December 1). Use of Force in Cyberspace. https://sciendo.com/it/article/10.2478/iclr-2020-0023

follow the rules of the 2015 GGE report, but the 2016/2017 GGE report had failed to achieve consensus due to many objections from state members on the use of force under Article 51 by arguing that it would represent the militarization of cyberspace. The 2019/2020 report had reaffirmed that IL and the UN Charter applies to cyberspace specially in situations of armed conflicts. [143]

Furthermore, it is important to realize that cyber operations can be considered as an armed force or an act of force because of several points. Even though they lack of traditional kinetic characteristics, cyber operations can have a same effect. One, based on the severity of the cyber attack. If the cyber operation conducted by a state or an individual threatens the state by harming its physical properties or has some sort of an extent form of coercion that can have a major impact then it is considered an armed attack. Cyber attacks usually have elements of severity because of its high technological use specially when dealing with data information. A state can have a highly developed system with highly developed hackers and individuals that could take any other state data and threaten it with a war attack or a terrorist act. Meaning that if a state could have important data that could take another state down it could cause not only physical harm but also economic also as states tend to threaten to have a huge economic deal which can severely cause economic losses to the targeted state.

Second, an immediate act of a cyber operation is made quickly which results in negative consequences by using coercion and threat the limitation to reach peace settlement would be reduced, which means that there wont be sufficient time to react to harmful consequences from a cyber attack, so it would constitute an act of force.

[143] Use of Force in Cyberspace. (2021). Congressional Research Service (CRS). https://sgp.fas.org/crs/natsec/IF11995.pdf

Immediate acts in cyber acts are highly common as the attacker usually tend to attack in a very rare time and day where it is not expected so that the state could not react fast which would get to the attacker's objective fast. This usually happens when the attacker tries to steal some of the economy of the state or important data that could harm the political independence of state. Acting fast can make the targeted state compel with the attackers demand since it has no other option.

Third, if the act of cyber operation was direct and linked to *actus reus* meaning that the state is consent of the attack causing harmful consequences then the prohibition on force is eliminated which results to be an act of force. Another point, a cyber act that is linked to be an invasion act that invades the territorial integrity of a state or its political independence, the act could damage a state which constitute an act of armed force and act of interference into internal affairs of a state which will cause an instability for the attacked state. Further, if the consequences of the cyber attack is easily identifies and there is a real result from coercion, then it is considered an act of force specially if the object is quantifiable. Finally, if the act is being resulted from violence and an act of responsibility done by a state then it will be characterized as a use of force which risks the international stability. Brief, a cyber operation or a cyber attack is to be considered an act of use of force which is unlawful under international law.

4.3.2.1 The non-intervention principle

Another principle of IL is the Non-Intervention principle which focuses on the prohibition to interfere into a states internal affair. This principle is not limited to the prohibition of threat and use of force in a state territory or political independence as indicated in the Article 2(4) of the UN Charter. The principle of non intervention means

that a state should not intervene in a dictatorial way of another state's internal affair. According to the Oppenheim's IL[144] for an intervention to be considered interfere, a state should intervene in a forcible way or coercive mean which can alter the control of the other state. If an intervention has pure and simple intention and means it is not to be considered an interference act. The principle of non-intervention came into context with Article 15 (8) of the Covenant of the League of Nations and the Montevideo Convention on Rights and Duties of States of 1933, which states that a state should not interfere with the freedom, sovereignty or any internal affair of a state or government of other nations.

The principle of non-intervention also applies to the external affairs of a state. A state should not intervene into another state affair unless the latter gives a permission. A state cannot intervene in any political, economic, social or cultural system of a state and specially not in its foreign policy, such any type of intervention is considered a wrongful act under IL even if the act is used without a method of coercion. For example, in the case of DRC V. Uganda, Nicaragua had clearly declared that the principle of non-intervention prohibits a state to intervene directly or indirectly, with or without the use of an armed force.[145] Also, in the Article 2(7) of the UN Charter, the UN is not authorized to intervene in matters of domestic jurisdiction of any state and members to the UN are required to follow the rules.

Further, the Vienna Convention on Diplomatic Relations, Article 41 had also established that diplomats should not interfere in any internal affairs of a state which is accredited to the state itself meaning that the state cannot interfere into the latter's

[144] JAMNEJAD, M., & WOOD, M. (2009). The Principle of Non-intervention. Leiden Journal of International Law, 22(2), 345-381. doi:10.1017/S0922156509005858
[145] (ICJ Reprts 2005, para. 164).

internal affair. The activities that the principle of non-intervention prohibits is the interference in political activities, a support of succession and the seek to overthrow a government by a regime change. These activities are considered unlawful and constitutes a breach of IL. When it comes to cyber context it is difficult to raise the issue of territoriality in an intervention matter since there is no physical space. However, if a state tries to use activities of cyber in any state it's considered to be a breach of the non-intervention principle even if there is an absence of ground.

A state usually tends to increase its interconnection to its society which results in an increase of their vulnerability to get manipulated, disrupted or attacked to its infrastructure system that supports its political, economic and social matter of its nation. However, sometimes vulnerabilities are available and can be exploited within another state. Cyber operations can have a similar impact as a military attack even though the results of a cyber attacks does not necessarily result in a physical damage to person but rather to the infrastructure system. Any attempt of a cyber attacks can be considered as an armed attack and a way of use of force. Since the Tallinn Manual2.0 has mentioned that the principle of sovereignty applies in cyber space as reflected in Rule 1, also the principle of non-intervention is an expansion of the concept of sovereignty, and according to Rule 66 of the manual, a state should not intervene into a state internal or external mean including by cyber means.

Cyber attacks are considered as a use of force as we concluded in the section before and an armed attack. The principle of non-intervention is one of the most elusive principles in international law. It is considered as potent since an intervention can intrigue countermeasures and it is an extension to the concept of sovereignty. It is

reflected in the rule 66 of the Tallinn Manual 2.9 which states that a state cannot intervene including by cyber means into a state's internal or external affair. Furthermore, the principle of non-intervention is considered a customary international law which is implied within the articles 2(1), 2(3), and 2(4) of the United Nations Charter and the Friendly Relations Declaration of 1970.

In order for the principle of non-intervention to be applied there must be two main conditions, one is the involving of internal or external affair of a state and second is the use of a coercive act by it's nature. Using cyber acts to coerce another state is considered a non intervention principle since the state engages in an intervention act by using force or an armed attack. This constitutes a wrongful act and enables the target state to respond with countermeasures. For example, in 2016 Russia had interfered into the U.S presidential election which is an example of a cyber intervention which is unlawful under international law.[146] The interference was by hacking the email system of the Democratic National Committee (DNC) and released mass information to the public which is considered a cyber espionage and a form of non-intervention.[147] Other examples were also seen in the UK, France, Netherlands and Germany which consisted cyber attacks on electoral infrastructure to manipulate the voting of an election.[148] All of these cyber attacks including the Russian voting interference had cause public harm meaning that it had harmed the democratic political process and value.

---

[146] Schmitt, M. (2021, April 19). The Netherlands releases a tour de force on International Law in Cyberspace. Just Security. Retrieved February 6, 2023, from https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/

[147] Ohlin, David. J, (2017). "Did Russian Cyber Interference in the 2016 Election Violate International Law?," 95 Texas Law Review 1579. https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2632&context=facpub

[148] Tsagourias, N. (2019, August 25). Electoral Cyber Interference, self-determination and the principle of non-intervention in Cyberspace. EJIL. Retrieved February 7, 2023, from https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/

It is important to discuss cyber interference in political matter like the voting system. The principle of non-intervention is fundamental in international law because it emanates from the principle of sovereignty. The meaning of non intervention is often associated with coercion since it falls under the category of internal and external affairs interference like political, economical, social and cultural system. The element of coercion basically implies a compulsion where the targeted state would be compelled by the other state against its will. If we want to basically look into the voting system interference some have argues that it violates the principle of self determination and not really constitutes a non intervention. However, looking at the nature of the act its important to take into consideration the consent of the targeted state. For example in the case of Russia, its obvious that it has the intuition of harming and altering the voting process of the presidential campaign in 2016.

Cyber espionage is a form of non intervention even if the coercion element is not quite explicitly seen. Coercion shouldn't only be physical harm or the type of use of force seen in a traditional attack, the cyber attack had targeted the political system of the state and had influenced peoples choice. Even if Russia did not force the U.S wills the element of coercion is there because that would have escalated into a major conflict. Thus, it had violated the principle of non intervention because this principle protects the aspects of self determination which is the right to choose and free expression. Since these rights were altered then it is a form of non intervention. Thus, there is the element of control which is a condition in coercion. The intervening state controls the people's cognitive environment of which government will be formed and their choices which is a form of non intervention.

Another example can be taken in the case of electoral system also. With cyber means it is possible nowadays to fake anything. Let's discuss the principle of non intervention during an electoral campaign that had images, voices and videos of politicians that were simulated meaning that what it was shown was fake. In this case, the authenticity and integrity of the information were being encroached which creates a confidential conflict. The fabrication information and the manipulation can alter the cognitive process of the forming authority and people's choice which constitutes a form of control over people's will and choice which is consider a form of coercion and a non intervention. Such cyber operations can violate the ideology of politics and an intervention into a state's affair.

4.3.2.1.1 Humanitarian intervention in cyber space.

Humanitarian intervention is one of the types of intervention when dealing with the internal and external affairs of a country. As we discussed in the title before, we have concluded that the principle of non intervention is illegal even when dealing with cyber means and methods. However, when it comes to humanitarian intervention will the case change? Humanitarian intervention under international law is the prevention or the stop of a mass violation of human rights in a state where the violation has risen to a war or a mass destruction and the state is unwilling to protect its own civilians or is actively persecuting them. In 1990, it was known as the year where the UN had allowed humanitarian intervention in many states. Even the SC had also authorize humanitarian intervention and we have seen the US and its allies also intervene for humanitarian reasons even when the SC hadn't authorize the action. Some other intervention were considered legitimate even if it wasn't authorized like the The North Atlantic Treaty

Organization (NATO's) intervention in Kosovo in 1999. [149]

Humanitarian intervention has been considered legitimate if the case scenario had scale to be very violent. However, one problem comes when dealing with humanitarian intervention which is the sovereignty of a state. In international law it's know that a state cannot violate the territorial sovereignty of another state and it should respect the integrity of the state and not interfere into its internal or external affairs. Article 2(4) of the UN Charter forbids the use of force or threat of use of force against either. The only exception is only when there is the right to use self defense under Article 51 of the UN Charter, and Collective Security measures under Chapter VII of the UN Charter. Some scholars had considered humanitarian intervention as legal and acceptable in international relations specially by the scholar Hugo Grotius who is also known as the father of international law. Some treaties and conventions had had and understatement that humanitarian intervention could be legal like the Genocide Convention 1948 encourages the permit intervention against genocide crimes. Based on its Article I, genocide crimes that are committed in time of peace or war is a crime under international law which they undertake to prevent and punish. The undertaking to prevent and punish can be understood here as either the authorization of use of force across state boundaries or limited set of measures like prosecuting and punishing. The treaties of the Organization of American States (OAS) and the African Union (AU) also encourages the use of collective force against their own member and is read as legal towards humanitarian intervention. [150]

Humanitarian intervention is a difficult matter under international law, till now the

---

[149] Jayakumar, K. (2012, February 9). Humanitarian Intervention: A Legal Analysis. E-International Relations. https://www.e-ir.info/2012/02/06/humanitarian-intervention-a-legal-analysis/

[150] Hurd, I. (2011). Is Humanitarian Intervention Legal? The Rule of Law in an Incoherent World. *Ethics & International Affairs, 25*(3), 293-313. doi:10.1017/S089267941100027X

debates still is on on whether it is legal or not because the main problem core is within the definition of Article 2 of the UN Charter and the principle of sovereignty. Even the ICRC had argued that international humanitarian law cannot be serve as a basis for armed intervention when there is grave violations and that it only applies when intervention forces are engaged in hostilities with one or more of the parties to the conflict.So the case is still on about the legality of humanitarian intervention. So how can be discuss its legality in cyberspace?

It is no doubt that cyberspace and artificial intelligence (AI) had increased the power of technology. When it comes to cyberspace and humanitarian aspect it can only be linked to the issue of nuclear weapons and systems which can cause a huge war and tremendous danger and violation if activated. In this case, it will be adequate to use humanitarian intervention and it wont be a matter of sovereignty or use of force but a matter of help. We have discussed before how cyberspace affects military basis and need, it can increase its vulnerability in its nuclear command control and communication systems that allows to detect cyberattacks. Cyberspace and artificial intelligence like nuclear systems can be activate through autonomous vehicles, remote sensing technology, munitions and even hyper-sonic weapons which is likely make a state to not survive a nuclear force.

The early Russian-Ukrainian war of 2020 had a lot of discuss of nuclear threats by Russia. Many policymakers had argued that Russia would deter the use of nuclear weapons through cyber operations. Some cyber experts have encouraged the U.S to use cyber attacks against Russia by considering a cyber “shock-and-awe demonstration” in response to a major Russian cyber attack against the West. A cyber action response like this could help NATO to prevent the fear of a nuclear war. In this example, we can

identify the use of intervention since the war in Ukraine had raised national security concerns for the United States and its European allies. The intervention here was seen as a matter of interference in another state internal and external affair and the use of economic coercive means against Russia. The U.S had also used cyber attacks against Russia and it was argued that the U.S had justified it's intervention for human rights reasons and to help Ukraine defend its state.

Regarding cyberspace, it is difficult to argue whether humanitarian intervention is allowed because it is not easy to detect humanitarian violations in the context of cyber attacks unless the attack was a nuclear war attack. The use of nuclear weapons through cyber operation should integer and allow humanitarian intervention since a nuclear war would destroy a whole complete state and would be a grave violation under international law. However, it remains unclear the legality of humanitarian intervention under cyber context since it is not yet a discussed subject by scholars and international law experts till now. Even though, this topic seems interesting to study and it would be a great benefit to the international law system if it there were many researches about it.

4.3.2.2 Cyber espionage and sabotage between states and the use of force.

Espionage is considered a very delicate matter under IL since it can have many breaches. International espionage happens when a state tries to access the information of another state that is confidential or strategic either in war time or peace time and this includes military, political and economic fields. Espionage has been for a long time ago a way to get into information through physical space, now in the 21st century it has changed to the field of cyberspace between state rather than individual or company to

company espionage. Not every kind of espionage falls under IL. Only those that is regulated by states under war or peace time and mostly during war time. It can also fall under human rights law specially after the 9/11 attacks[151] which made states implement more surveillance programs to fight terrorism. Many specialists like Edward Snowden, an agent from the National Security Agency (NSA) have argued about the legal and political implication of espionage under IL. Some other specialist have argued the fact that espionage can be legal under international human rights law.

The reasons why espionage is a complicated matter under IL is that cyber espionage or espionage between states in general is sophisticated because of the set of rules that a state can face from sovereignty, nonintervention, the use of force, human rights, international economic law and international criminal law. So, it is hard to identify the legality of cyber espionage because of these set of rules. However, according to the majority of IL specialist espionage in general can be legit since there is no rule that says the opposite. Cohen-Jonathan and Kovar 1960 have noted that there is no rule about espionage between states even in time of peace.[152] Moreover, Kish and Turns 1995, Lafouasse 2012, and Chesterman 2006 also concluded the same this emphasizing that espionage should be looked into the rules of human rights, humanitarian law, or also diplomatic law.[153] By contrast, the minority of IL specialist have concluded that espionage is in fact prohibited under IL. Specialists like Wright 1962 (cited under Espionage and Sovereignty), indeed, argues that espionage can be a

[151] The September 11 attacks, commonly known as 9/11, were territost attacks that were coordinated and carried out by the militant Islamist extremist network al-Qaeda against the United States on September 11, 2001

[152] Dubuisson, F., & Verdebout, A. (2018). Espionage in international law. oxford bibliographies. Retrieved February 7, 2023, from https://www.oxfordbibliographies.com/display/document/obo-9780199796953/obo-9780199796953-0173.xml

[153] IBID,152

breach to sovereignty and a violation of nonintervention. [154]

Because of the several opinions about espionage, it is considered a legal sensitive issue because it involves ethics and political matter which makes espionage an uncertain matter under IL. However, it is important to analyse espionage during war and peace time to conclude the legality of cyber espionage under IL. If we want to analyse the legal effects of espionage during wartime, it is essential to look at the status of a spy. It is known that a spy is an agent considered a belligerent that gathers information from the opposite side with the intention to give it to the first side which is the attacker. Under the treaty and customary IL, spies do not enjoy prisoner of war protection and the reason is because they fall under the status of criminals and they are convicted if captured. However, espionage is not really fully considered illegal under international humanitarian law since it has not declared the opposite even though spies can be seen as combatants that commit unlawful acts. During peacetime, espionage becomes more ambiguous as there is no treaty that regulates the use of spies and it is even difficult to determine its legality under IL.

Another point to consider is whether cyber espionage would constitute a breach under the UN Charter. Article 2(4) of the Charter states that all members should not use threat or force against a state territorial integrity or political independence, this article establishes the principle of non-intervention under IL and any state that breaches this rule would breach the Charter as a whole. However, when dealing with espionage or cyber espionage it would involve the presence of agents at another state's territory and in the case of cyber espionage it would be the absence of the agent but in the territory of the opposite state. So, these two conditions whether cyber or physical would still be a violation of the non-intervention principle under the UN Charter, which could be

[154] IBID,152

consider an international crime. In contrast, espionage and all its forms including cyber espionage could be seen as a tool of diplomacy as it is consider as an intelligence service that thanks to it states can solve and regulate complex as well as an international relation way of communicating and an interest to not use force which makes it harmful to doubt whether it breaches the principle of Article 2(4) or not.

Moreover, espionage and cyber espionage could be seen as a way of self defence and an alternative way to not use force which can also cause doubtfulness when examining its legality under UN Charter framework. Since the main purpose of cyber espionage is to collect information of the targeted state by using computer and internet, its purpose is not clear under IL and there is a difference between a spy and a diplomat. The main difference is the fact that an spy would not disclose its status and will remain anonymous unlike a diplomat that is known to the receiving state. Also, spies do not try to make conciliation or make developments to the receiving state, so it is not seen as a target state. Another point, is that diplomats have to use peaceful means and ways while dealing with the state unlike a spy that can use unlawful means to exalt the job. So to conclude this idea, it is hardly to consider cyber espionage a form of diplomacy which takes us to the main idea, that it is a breach of the UN Charter because of its unlawful means and methods.

Another point to discuss is that international law establishes a principle called Estoppel which prohibits states to go back to their previous statements or conduct if their actions were to be relied upon another state[155]. So this principle could be challenging in matter of espionage and cyber espionage since it is difficult in determining its legality on the basis that espionage is practiced in a widespread arena in

[155] Gavin, D. (2022). Estoppel. Jus Mundi. Retrieved February 7, 2023, from https://jusmundi.com/en/document/publication/en-estoppel

the accusing state which includes reliance on the challenge states. On the other hand, diplomatic law gives states the power to unilateral declare diplomats as *personae non grata* if they interfere into other states internal affairs, so if a diplomatic engages in spying act he or she could claim to use intelligence service as a diplomatic act, however it is not a good idea since states can declare him an unwanted diplomatic agent in the international community. To add more, in the Tallinn Manual has also mentioned that cyber espionage could be a way or cyber attacks which could lead to a cyber warfare, so using surveillance systems can also breach the non intervention rule, sovereignty and political independence of a state even if it lacks coercive physical elements, since states need should not be breached by its physical or virtual barrier.

4.3.3 self defense in cyber attack context.

The principle of self defense under international law is referred to the right to use force in case of self defense against an attack from another state. It is defined as the use of force as a direct attack against oneself or another state to repel an attack or the threat of an attack. The self defense case is considered an exception that should be use when there is a situation that could endanger the security of the other opponent. Under Article 2(4) of the UN Charter the use of force is prohibited as discussed earlier before. However, when there is a situation where a state should either attack or get attacked, it will use force as a shield to get protected which is considered lawful among scholar under IL. The concept itself is also used in criminal law as a defense to justify the use of force, so why not also use it among states. According to Article 51 of the UN Charter, there is nothing that should impair a state the right to use self defense when there is an armed attack that occurs against a member of the UN. By that being said, attacks

justified by self defense is considered lawfully under IL. However, the question involves a constant debate regarding the applicability of self defense in cyberspace. [156]

In regards to cyberspace, if we want to take into consideration Article 51 of the UN Charter, then the use of cyber attacks as a self defense is justifiable under the article. However, the dilemma is involved when not considering a typical cyber attack as an armed attack. It is notable that under IL only those attack that result in significant damages are considered an armed attacked. If a cyber attack does not result in significant damages and consequences like death or destruction, would the self defense principle be applied?. [157]

An analysis could be made regarding the situation of elf defense in cyberspace. Lets take a fictional example. If supposedly state A has the constant will and consent to use force against state B by applying a ransomware attack to a governmental place for example the MOFA[158]. State A had attacked data from the other state and had steeled many information that could put into risk state B national security. The targeted state had been aware of the attack and applies a cyber operation against state A by attacking its governmental infrastructure system. This case is considered lawfully since state B had acted in self defense against state A who targeted it first and had cause some damages.

However, if the case scenario is different and state B instead of attacking the infrastructure system of state A as an act of self defense it decided to attack a

[156] Carlo Focarelli, 2015. "Self-defence in cyberspace," Chapters, in: Research Handbook on International Law and Cyberspace, chapter 12, pages 255-283, Edward Elgar Publishing.
[157] International cyber law: interactive toolkit. (2022, September 12). Self-defence. International Cyber Law: Interactive Toolkit. https://cyberlaw.ccdcoe.org/wiki/Self-defence

[158] Minestry of Foreign Affairs

government building meaning a ministry, and during the cyber attack, the operation resulted in deaths of people who were in critical states, could this be considered an act of self defense?. If we want to be sincere and deeply focused, it is to be argued that if the state was consent that it is going to attack a ministry and that the cyber attack could result in deaths then this is not considered an act of self defense but an act f use of force and state B can have serious consequences as it had cause significant damage to a civilian which is prohibited under IL. The cyber attack in this case could be qualifies as an armed attack which is prohibited under IL. If the attack was made by accident or the state was not fully consent that it could cause serious injuries and deaths it would be difficult to considered the act as a self defense act because the state B had intentionally attack a ministry regardless if it had the consent of the after math or not. If the act was to be considered as a self defense act then state B would have attacked state A with a similar cyber operation without resulting in deaths against civilians. By being said, the act of self defense is considered lawfully unless the act had malicious intentions and had cause significant damages to civilians.

4.3.1.1 Principle of proportionality in context with cyber operations.

The principle of proportionality is an important matter in IL and it prohibits any attack that could cause a loss of a civilian life, an injury or a damage to a civilian object which is mentioned in Article 51(5)(b) of Protocol I of the 1977 Geneva Conventions. It has also been defined by the ICRC Study as a rule of customary international humanitarian law that is applicable in international and non international armed conflicts. If a state or an individual violate the principle of proportionality regardless of the amount of violation it constitutes a war crime in an international armed conflict

under the Rome Statute of the ICC. Thus, the principle is also applicable when a military object is being attacked. In essence, causing harm to civilians and civilian objects can be unavoidable in cases. However, it doesn't not mean that the principle wouldn't be violable. [159]

Since proportionality is an important core in international law, it provides elements of legality for an action of what is permitted or not depending on the objective and means and methods of an attack. This principle tries to balance between a military necessity and the legality of the use in an armed force. It applies in cases of self defense and in cases where a states is restoring the order of an internal disturbances as well as in situations of international and non-international conflict. IL is known as the legal body that allows states to only use force in self defense cases. In the UN Charter of 1945 incorporates measures that are proportional to an armed attack and the necessity to respond to it. Also, IHL uses the principle of proportionality to limit the damages that is caused by military operations towards a civilian individual or a civilian object. [160]

If we want to discuss the principle of proportionality and its applicability in cyberspace, its important to explain how this topic was first discussed. In 2016, in a thematic round table held at the Humanitarian Centre in Moscow,[161] experts have discuss this topic specifically for the first time. The event was organized by the International Committee of the Red Cross (ICRC), the PIR Centre and the Institute of

---

[159] Gisel, L. (2016). THE PRINCIPLE OF PROPORTIONALITY IN THE RULES GOVERNING THE CONDUCT OF HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW. INTERNATIONAL EXPERT MEETING. https://www.icrc.org/en/document/international-expert-meeting-report-principle-proportionality#:~:text=The%20principle%20of%20proportionality%20prohibits,and%20direct%20military%20advantage%20anticipated.

[160] Doctors without borders | The Practical Guide to Humanitarian Law. (n.d.). https://guide-humanitarian-law.org/content/article/3/proportionality/

[161] "Weapons and the International Rule of Law ", the 39th Round Table on Current Issues of International Humanitarian Law (Sanremo, 8th-10th September 2016).

Information Security Issues (IISI) of Lomonosov Moscow State University. Many experts from different countries have issued the matter and concluded some results. Many arguments have been added to the discussing including the fact that the principle of proportionality is referred to a collateral damage which is inevitably subjective. Other arguments have added that states should be responsible for its civilians which means that they have to put effort in exercising caution and prevent any unnecessary loss of a civilian in a hostility rather that calculating the percentage of loss. Further, another expert have added that the principle of proportionality should be taken seriously and into account regardless of the result. [162]

In a cyber context, when a cyber attack happens the result is different from an ordinary attack. If we want to evaluate the level of destruction, both have same levels regardless of the method and weapons used in a hostility whether its from a cyberspace or from a kinetic war. Since IHL and IL applies to cyber attacks and operations then any rule is applicable to a cyber attack situation. If we want to understand an attack as a destruction whether its physical or not, then the principle of proportionality applies to cyber attacks if the act had resulted in serious damages. If a cyber weapons was used as a military objective and it harmed a civilian which resulted in death for example, then the principle of proportionality would be applicable in this case. The case is about protecting civilians and their objects so attacking an individual's computer in a cyber war would constitute a breach of IHL.

[162] Moscow, I. (2018, February 16). Cyberspace operations in armed conflicts and the proportionality rule. Humanitarian Law & Policy Blog. https://blogs.icrc.org/law-and-policy/2016/06/29/cyberspace-operations-armed-conflicts-proportionality-rule/

4.3.1.2 Basis of necessity under IL and the application in cyber context.

The basis of necessity is an important subject under IL and customary international law specifically and it has been codified in the Article 25 of the International Law Commission (ILC)'s Draft Articles on State Responsibility. States should invoke the basis of necessity during a crisis as an excuse for a breach on an international law obligation. Applying the basis of necessity may lead a state to a position where it cant consider its conduct wrongful. This concept is considered important because it regulates the circumstances in which an abrogation of an obligation is excuse. It means that a state can escape from a responsibility by excusing itself based on a necessity circumstances. For the basis of necessity to be considered successful it must have an exceptional nature, meaning that if a necessity defense would be applicable, it must meet the requirements for it to be applicable. [163]

However, if we want to analyse whether the basis of necessity can applicable under a cyber context, its important to know when its considered legitimate in application. This basis is considered legitimate if a state excuses itself for applying it because of a matter that had breach its security interest or the internal peace of the state. If a state would apply the basis of necessity the act should have an essential interest against a peril that is grave and imminent. Necessity in a act of justification by states which is used in order for a state not be deemed internationally wrongful. In a cyber context, if an offensive cyber capability is deployed against another state, the latter would invoke the basis of necessity when there is a serious threat to the state interest.

[163] Mundi, J. (n.d.). Wiki Note: Necessity as a Defence. https://jusmundi.com/en/document/publication/en-necessity-as-a-defence

Thus, the basis of necessity would be invoked if there is also an interest for a state to apply it in case of threat. If the damage was imminent and objectively verifiable, then the basis of necessity is applicable. Also, there isn't a specific degree of damage that would be sufficiently serious to justify the need of necessity. In cyber context, since the damage is not always physical, situations where the internet is inaccessible or where there is severe shocks to a financial market, evoking the basis of necessity would be justifiable since the attacks was made virtually and the options for taking an action is limited. This would give the state the opportunity to protect its own interest and minimize the damage.

4.3.4 Jurisdiction of cyber attacks.

In Public International Law the concept of jurisdiction is linked to the concept of sovereignty, and as explained before in the previous sections, a state cannot violate the sovereignty of another state and its sovereignty is only extended within a state territory. Having jurisdiction means that a state will allow to have a sovereign independence which it can pass on with the global system which makes it important for the international order. When it comes to IL it addresses the international criminal law mainly through the ICC. IL can have a perspective jurisdiction over a territory, nationality or in cases where it needs to protect the national security of a state. [164]

The ICC can have only jurisdiction over crimes that are defined as war crimes, crimes against humanities, genocide, and crimes of gravity that can lead to one of the crimes mentioned before as its stated in the Rome Statue. Also, its important to note that

[164] Donovan, D., & Robert, A. (2006). NOTES AND COMMENTS THE EMERGING RECOGNITION OF UNIVERSAL CIVIL JURISDICTION. Law Yale. https://documents.law.yale.edu/sites/default/files/Donovan100AmJIntlL142[1].pdf

the ICC can also prosecute and investigate natural persons meaning that it only has jurisdiction over nationals from a state and not governments, corporations or political parties.

The International Court of Justice known as the ICJ was based on the Hague Conventions in 1899 and 1907[165]. In 1913 it was known as the Permanent Court of Arbitration. After the First World War it became the Permanent Court of International Justice and even though the court wasn't active after the Second World War it become more effectively after. It was established by the UN Charter and all members who are part of the UN Charter are also part of the court. The court consists of 15 judges who are elected for 9 years by the UNGA and the UNSC. One third of the judges are selected each 3 years by an election. The court applies International Law principles when dealing with cases. The court can give advisory opinions on any legal questions only by a request of the organs of the UN. The court decisions on any case are considered final and without appeal. The International Criminal Court (ICC) is a bit different since it has only jurisdiction over crimes related to IHL. The court is a legal body of IL that was established by the Rome Statute[166] of the ICJ in 1998 to investigate crimes of genocide, against humanity, war crimes and punish those who are responsible. [167]

Both courts are important legal bodies under IL which can be taken as references when dealing with war crimes. If we want to analyse cyber operations, cyber attacks and cyber warfare under this section its important to ask whether cyberattacks can violate

[165] The Hague Conventions are international treaties and declarations that were a result of international peace conferences at The Hague in Netherlands. This is the first formal treaty along with the Geneva Conventions that treats the law of wars and war crimes under international law.

[166] The treaty of the ICC.

[167] Britannica, T. Editors of Encyclopaedia (2022, May 3). International Criminal Court. Encyclopedia Britannica. https://www.britannica.com/topic/International-Criminal-Court

IHL or not. To understand more, its important to highlight that cyber operations work under an umbrella of cyberspace. The term cyber operations covers every activity that involves *inter alia* cyber espionage, cyber manipulation including cyber attacks. If we want to think about cyber operations under international criminal law we wont get a result since cyber operations are not considered aggressive as cyber attacks. It we want to investigate under international criminal law, its more convenient to analyse cyber attacks under this domain.

Cyber attacks can lead to a breach of IHL and considered an international crime if an only the results of the cyber attack were aggressive and it led to harm civilians. If the attacks was risen to be a cyber warfare which deals with military activities to achieve military objectives by using cyber weapons, then the cyber attack can cause injury, deaths and damages to objects or its destruction. By that means, a cyber attack can be an international crime if the attack was grave. So for the ICC court to have jurisdiction over a cyber case, the cyber war must be considered an armed conflict under Article 2 of the Geneva Conventions.[168] If the cyber attack led to a warfare because of the use of strong cyber weapons that could almost have the same effect of a kinetic weapon then it can e considered an international crime.

If we want to look at this perspective, we can note that the ICC is more adequate to apply in cyber attacks and cyber warfare because it can prosecute individuals. In contrast, the ICJ is only applied when two states are confronted to each other. This is why, the ICJ has not been delivered a cyber case till now.

[168] Common Article 2 to the four 1949 Geneva Conventions provides that they 'apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them'

In cyberspace or cyber technology it is interesting to look which legal body has jurisdiction over cyber attacks or operations. However, the ICC has receive little attention over cyber criminality and even the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations only devoted 2 rules out of 154 to cyber international criminality which falls under the ICC's jurisdiction and this occurs when the cyber attack is associated with kinetic weapons and involve elements of war crimes listed in Article 8 of the Rome statute and the second is if the act was committed in the territory of a state party and involves gravity. But, in spite of that states have been actively interested in addressing cyber criminality even though it was ignored by the Rome Statue and was not included in the final version of the treaty. If we want to analyse whether a cyber malicious act falls under the jurisdiction of the ICC or not its important to analyse the conduct of the cyber act. If the conduct constitutes a crime that integers new ways to commit it then the ICC has jurisdiction under its Statute and if the act facilitates the commission of the crime it also falls under its jurisdiction.

Further, a cyber attack that is conducted by a belligerent in an armed conflict and has a malicious intention of harming a civilian o destroying civilian objects which can result in a loss of life, injury or long term damages would amount to war crimes under Article 8(2)(b)(i), (ii) and (iv), and Article 8(2)(e)(i) of the Rome Statute.Indeed, cyber attacks or operations in its nature have the ability to produce physical damages in the operating system of a physical infrastructure and it can result in a malfunction of the infrastructure that can possibly cause a loss of life or a destruction of a property. For example, if a belligerent tries to manage a cyber attack by shutting down the cooling system of a nuclear power which is located in the territory of the opposite opponent, and it causes radioactive release that aimed civilians this falls under the ICC jurisdiction and

constitute a cyber criminality type of act.

Furthermore, cyber attack attack that have a serious and harmful physical consequences or towards an individual can lead to a genocide or if the attack was committed as part of a systematic attack that aims directly against a civilian population with the intention of attacking and committing a crime against humanity whether it was occurred within the context of an armed conflict or not can also have apply under the ICC jurisdiction. Sometimes, a cyber attack can reach the level of a crime of aggression as it is provided in the Article 8 bis (2)(b) and (d) of the ICC Statute,which refers to any attack that is made towards a state by an armed force on land, sea or air forces, or marine and air on other states. By that being said, a cyber tool can be used as a war weapon to cause harm. In order for a crime to be reach a level of criminality liability it must be grave and scale by its character. [169]

Another interesting point is the crimes that undergo in Article 7 of the Rome Statute specifically point (g) which refers to crimes that are related to sexual slavery and rape, including enforced prostitution and sexual violence which all are considered as a whole as a crime against humanity. It is widely know that one of cyberspace crimes is sexual cyber activities that can occur inside a state or outside another state. Let's say state A had been engaged in a cybercrime using a non state actor, either an individual or a state representative and had been forcing other individuals from state B to do sexual slavery and enforced prostitution, would the ICC have jurisdiction over the case? Does this constitute a direct cyber war or not?

[169] Rocisini, M. (2019). GRAVITY IN THE STATUTE OF THE INTERNATIONAL CRIMINAL COURT AND CYBER CONDUCT THAT CONSTITUTES, INSTIGATES OR FACILITATES INTERNATIONAL CRIMES. Criminal Law Forum (2019) 30:247–272. https://link.springer.com/content/pdf/10.1007/s10609-019-09370-0.pdf

The answer to this question could vary depending on the case. If state A had engaged in a malicious cyber operation against state B by enforcing cyber sexual crimes, then in this case it constitutes a crime against humanity according to Article 7(g) and the ICC would have jurisdiction to prosecute the individuals involved in the cyber crime. Another case scenario would be that State A had given the power to certain hackers individuals to make a direct attack on governmental military officers by hacking the system and making military officer of female sex from state B do forced prostitution by the act of threatening and attacking the whole system and causing an attack as a whole which would result in deaths or damages, if these military women had no option but to proceed with the threat and protect their country, in this case it would constitute a war crime meaning a cyber war crime under Article 8 (2) of the Rome Statute which also constitutes a a serious violation of article 3 common to the four Geneva Conventions. In this case the ICC has the right to prosecute these individuals and have jurisdiction over the case unless these individuals could not be found anywhere and they were anonymous which is highly like to be the case in cyber crimes because it is difficult to detect who was behind the attack which makes it even harder for the ICC to proceed.

In case where the attack was an explicit cyber attack from state A to state B like in the case of the Ukraine-Russia war of 2022. according to CSIC the cyber war between Ukraine and Russia had begun since 2014 but it was seen more in the last war between these two countries. The cyberattacks was against Ukraine trying to destroy and damaging the infrastructure system and data in the 2022 war. Russia had launched a cyber campaign which constituted an invasion which resulted in a huge increase of exploits. The cyber intent had managed to attack directly the Ukrainian state by disrupting services and installing malware on networks by using phishing, denial of

service and taking advantage also of the vulnerability of the system. The cyber attack resulted in targeting governmental websites, energy and telecommute service providers as well as financial institutions and media outlets. One of it's most successful Russian cyber attack on Ukraine was the Viasat Inc's KA-SAT satellite.

The case above is an example of a direct attack from a state to another state by cyber means. This constitutes a violation of Article 1(4) of the UN Charter which prohibits states from using force and threat in their international relations.

4.3.5 Neutrality principle according to technology and IHL.

4.3.5.1 The concept of neutrality in the context of technology.

It is important to acknowledge the importance of technology in our lives today and how it needs to be developed according to the development of the society technology is an important part for society either for individuals organizations or States everyone has the freedom to choose how they can use technology in the most appropriate and suitable Way for their needs in every life either to use it for politics or for commercialization or for any kind that needs data and information.

According to the value neutrality thesis, the use of technology is considered as morally and politically neutral and accepted which means it's not considered good nor bad. Technology depends on humans intentions either using it by an individual or by state which means that an action should be freely choose by the user regardless of the reason. Further according to the technologist Mauro D. Rios he proposed some principles for this concept is to have the freedom of opportunity to use technology in

public sector or private sector or academic. To have a dependency using technology with its services and its freedom to interact with other persons or organizations by electronic means without being imposed *de facto.*

Regarding technology neutrality it is a concept to be considered for a state. A state cannot impose preferences with or against technology. User can freely use whatever they think they need from a network to a service without specifying. The principle of neutrality sets the rules for how to use technology. If the use of technology is harm and causes local or international problems it might have consequences for the user that tries to abuse the use of technology. However, the use of this principle applies to technical means not to ethics or social issues. For example, when a state wants to adopt a rule about free software to restore the computing sovereignty of a country which basically will let people have freedom and cooperation, this is not a technical matter but rather a social and political one, which means that the state shouldn't be neutral about it because it's not a technical thing.

4.3.5.2 Neutrality principle under the context of international law and IHL.

The law of neutrality is an important subject under international law, it defines the legal relation between states when engaging in an armed conflict and those who are not taking part of a hostility. Neutrality is described as a position that a state takes which refers to it's nonparticipating and it's non-engaging in an armed conflict in which it does not want to become involved. This principle serves as a way to localize war and conduct its limit on land and sea to minimize the impact of war. When a state is defined as neutral it means that it has proclaimed its neutral status. The law of neutrality acts as a defense to protect the sovereignty of a state to prevent any escalation of an arm

conflict. [170]

The principle or law of neutrality is specified in international treaties. For example, in the Geneva Conventions, it has mentioned terms like ‘neutral Powers’, ‘neutral countries’ or ‘neutral States’. Article 5 of the Geneva Conventions is an example of the application of neutral powers in which it regulates situations in which persons protected by the Second Convention are in the territory of a neutral Power. Thus, Article 15 of the 1907 Hague Convention (V) also deals with the applicability of the law of neutrality to land warfare. It is also states that the law of neutrality applicable to land warfare is also referred to the applicability of the Geneva Convention.

A state that takes a neutral positions means that it does not want to take a side in a conflict. The concept of neutrality was associated to international politics and then it was developed to staying outside of military alliances and conflicts of other states. A neutral state does not take a side in a hostility and it abstain itself from committing hostile acts or giving military advantage to a party of a conflict. In addition to the four 1949 Geneva Conventions and Additional Protocol I of 1977, various other international conventions address the issue of neutrality like the La Hague conventions, example, the 1907 Hague Convention (IV) in Respect to the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land; the 1936 London Procès-Verbal Relating to the Rules of Submarine Warfare Set Forth in Part IV of the Treaty of London of 22 April 1930.

Customary international law also provides an option for states whether they want

[170] The Law of Neutrality. (1999). International Law studies-Volume 73. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1558&context=ils

to participate in an armed conflict or not and the right of declaring a neutrality status. The law of war imposes rules and regulations for both belligerents and neutral states even if not wanting to participate in a war. Further, the Charter of the UN imposes its member the obligation to settle international dispute by peaceful means and the prohibition of use of force in any international relations matter. If a breach occurs, the Security Council will take enforcement actions on its members to maintain peace and order. It is an important matter to note that the law of neutrality protects the territorial sovereignty of a neutral state and on the other hand it also protects the belligerents interest against any interference from a neutral state.

When applying this principle to cyberspace, it does not change from a traditional war. A neutral state does participate in a hostility in any way whether it was by using kinetic means or cyber means. Thus, it is important to note that neutrality law applies when cyber operations or attacks take place by the use of a cyber infrastructure which is located withing the territory of state that is neutral. Which means that belligerents must respect the limit of a neutral state and its prohibited to exercise any belligerent action withing the territory. However, the problem involves around the cyber activities that are committed through neutral cyber infrastructure, it is not clear yet whether the prohibition also applies to it or not. [171] It is to conclude that this principle protects the cyber infrastructure which is located in a territorial of a state. On the other side, neutral states must also respect the principle by not engaging in any cyber activities that could support military activities.

4.3.6 Simplicity of cyber attacks and collateral damages.

[171] von Heinegg, W. (2012). Neutrality in Cyberspace. 2012 4th International Conference on Cyber Confl Ict. https://ccdcoe.org/uploads/2012/01/1_3_von_Heinegg_NeutralityInCyberspace.pdf

Collateral damages under international law are defined as incidents that resulted in death or serious long term injurious as well as destruction to a civilian object. Based on article 51(5)(b) and article 57(2)(a)(iii) of the Additional Protocol I (AP I) of the Tallinn Manual, a cyber attack may result in damages and injurious as well as loss of lives which would be described as a collateral damage. In order to determine the status of the injury of the incident there needs to be an evaluation of the harm and compare them with those of direct military attacks in a combat field. Under Art. 57(2)(b) of AP I, if a cyber attack had a collateral damage consequence, the attack must be canceled or suspended. It is important that the state or the individuals chose the right method and mean of cyber warfare or cyber operation to minimize any damages to civilians and their objects based on art. 57(2)(ii) of AP II (see also Rule 55 and 56 of the Tallinn Manual).

Moreover, states and individuals must have an obligation to chose the adequate target while using cyber operations which will create less danger to civilians based on art. 57(3) of AP I (see Rule 56 of the Tallinn Manual). Direct attacks to civilian and their objects and properties is considered prohibited unless it was the case of dual use then an assessment of necessity is gained. In cases where there are mercenaries for example, they are to be considered as belligerents but without combatants privileges. In a case where a civilian participates in a cyber operation that would cause a collateral damage or even the minimum damage, then it loses protection, and this also applies to those that participate in a *levée en masse.*

Another point to outline is the cyber attacks which takes place against works and installations that could contain serious forces especially if it contains dams, dykes, and

nuclear electrical generating stations, as well as installations located in their vicinity (see Rule 80 of the Tallinn Manual, based on art. 56 AP I and art. 15 AP II), these are to be considered prohibited. Also, attacks that have the intention and object of causing terror among civilians is also prohibited. If a cyber attack result in removing objects that protect civilians then it is also considered unlawful especially if the attacks targets medical personnel, medical infrastructures, medical computer and networks, personnel and objects of third parties to the conflict trying to provide humanitarian aid and objects necessary for the survival of civilians.

In addition, in order to define if a cyber attack is consider simple or not, its important to see the different types of cyber attacks. First, it could be a cyber attack that is aimed directly to a target which can aim a civilian too and cause collateral damage. This is consider as a cyber attack which is not simple due to the consequences that resulted because of the attack. Second, an attack where the aim is directly to targets but it attacked civilians because it was difficult to distinguish between them in the attack, this would make it still prohibited and a cyber war regardless of the intention. Finally, a cyber attack that involves the targeting of everyone with the intention to cause a war and collateral damages regardless whether it hits the aimed target or civilians, in this case the attack would not be considered simple and it can result in collateral damages.

4.3.6.1 Military, civilian objectives and collateral damages in the context of cyber attacks.

International law and International humanitarian law had distinguished between civilians and military objectives. Article 5 of the Protocol of the 1977 Geneva Conventions had defined civilian objectives are those that are excluded as combatants.

Article 3 (7) of the Protocol had also provide the protection of civilians unless they take a direct part in a hostility. According to the IHL rules, civilians and their objects cannot be a direct target and parties should distinguish between civilian objects and military objectives. Military objectives are those objects that are used in a military armed force which includes weapons and military equipment and they make contribution to the military service. [172]

In an armed conflict, protecting civilians and their objects should be a duty and a responsibility of military commands as well as a moral and legal responsibility. In this means, military activities should not contribute to a total or partial destruction that leads to a collateral damage. The U.S. Department of Defense (DoD) defines collateral damage as an*"unintentional or incidental injury or damage to persons or objects that would not be lawful military targets in the circumstances ruling at the time".* Thus, the Program on Humanitarian Policy and Conflict Research at Harvard University had also defined collateral damages as those that reach to a loss of a civilian life or injury and damage to their objects caused by an attack or lawful target. [173]

In an armed attack, there should be a distinguish between civilian and military objectives, however, in many cases collateral damage can happen with the intention of damaging or without the consent. For example, in a military attack, there was damage in a military command center and a civilian school by a kinetic mean or a cyber mean.in this case, the damage in the civilian school is considered a collateral damage but the damage in the military command is a side effect of the attack which is considered a military advantage to the attacker and is not considered collateral damage since it is an

---

[172] و. شعيرة بن .(2018) .القصف وعمليات الإنساني الدولي القانون :المفرطة الجانبية والأضرار المشروعة العسكرية الأهداف .للدراسات الباحث مجلة الأكاديمية, 5(2), 673-687. https://www.asjp.cerist.dz/en/article/59698

[173] Romanosky, S., & Golman, Z. (2018). Understanding Cyber Collateral Damage. JOURNAL OF NATIONAL SECURITY LAW & POLICY [Vol. 9:233]. https://jnslp.com/wp-content/uploads/2018/01/Understanding_Cyber_Collateral_Damage_2.pdf

accidental harm. However, in the case where the outcome of the attack was subsequent harm as a result of any retaliation in any form such as diplomatic, informational, military, or economic (sometimes referred to as “DIME”)then it is not considered a collateral damage but rather a violation on the law of war.

In a cyber context, the definition of collateral damages has the same outcome. A cyber collateral damage is defined as a unintended harm to a computer or information system which is not target to a lawful cyber operation. In this case, an unintended harm is considered as a manipulation, deletion or alteration of a computer code that governs the operation of the computer hardware or software that is not specifically intended by the party conducting a lawfully-authorized operation. For example, in 2003 during the Iraqi war, the U.S military had destroyed the communication systems of Iraq physically and it had disable satellite and other communication equipment that provide assistance to the Iraqi military force and to the civilians in Iraq and its neighboring countries.This was an example of a cyber collateral damage as these communication equipment were giving assistance to civilians and it who were not part of the hostile. In 2008, a similar case happened when Iraqi severs were also destroyed by military cyber operations which also impacted the internet connectivity and IT systems of computers in Saudi Arabia, Germany, and Texas. Both examples show signs of collateral damages to civilian communication.

To conclude, cyber collateral damages in a military activity are considered unlawful and against the rules of IHL. In a military attack, cyber operations and attack that affect civilian communications are considered against the law and a violation to IHL. Military objectives should only be within the context of the military activity and a

cyber operation and cyber harms should only be against the military of the targeted state and should exclude any civilian life and objective to avoid collateral damages.

4.4 International security and state's responsibility towards cyber attacks damages.

According to the Responsibility of States for Internationally Wrongful Acts of 2001, article 1 it states that : *" Every internationally wrongful act of a State entails the international responsibility of that State."* This article is important because it emphasizes that a state should be responsible of any wrongful act that is committed under its territory. A state can only be held accountable for an international wrongful act if the act itself was attributed to the state by laws and regulations of the IL and if the act constituted a breach of a state's international obligation. A state can be in a culpable situation if a wrongful act committed by the state was a violation of another state's sovereignty or territory. A state can also be held accountable if it breaches rules committed within an international institution even though these acts are defined by the domestic law of the state.

Another important idea to point out is that a state is also responsible of its civilians meaning that it is responsible of private acts that a person can commit within the territory of a state. For example, in 1979 Iran supported the seizure of the U.S embassy by holding the militants, diplomats and other embassy staff as hostages. However, some acts like this can be justified as a peremptory norm of IL and a self defense method under the UN Charter if the act itself had an intention to pressure the opponent state with its international obligations. Further, a state must take full responsibility of an illegal act that had cause injuries and it must repair and restore the situation if possible and offer compensation when needed as a matter of satisfaction.

Furthermore, according to a suggestion made by the International Law Commission in its 1996 draft on State Responsibility, that states can be held responsible for “international crimes”, which includes acts related to colonialism, aggression and genocide. In addition, in 1980 in the U.S Vs. Iran case, the ICJ held that the actions of the citizens could be attributed to the government if they acted on behalf of the state. However, the court didn't find evidence to affirm this, even though the court had already found Iran responsible of the actions because it was aware of the obligations under the 1961 Vienna Convention on Diplomatic Relations and the 1963 Convention on Consular Relations to protect the U.S. embassy and its staff.[174]

In a cyber context the rules does not change, a state can also be responsible of a malicious cyber conduct that is conducted within the territory. It is also applicable in the field of IHL, as cyber weapons are considered weapons of war and they are qualified unlawful if causes harm and damage. In case where a certain state has been attacked by cyber means, the state should always respond with countermeasures. If the state has been the victim and suffered from losses then the attribute of the attack is given to the state that contributed the cyber attack. Also, according to the IL rules, a state can be responsible for the actions of its agents or civilians in case where the attribution was given to the state in an international wrongful act which constituted a violation of an international obligation.

In addition, according to the Common Article 1 to the Fourth Geneva Conventions, a state should ensure that it follows the rule of laws of war even if it was the attack state or the targeted state. Hence, if a violation occurs, the injured state should take measures

[174] Schackelford, S. (2010). STATE RESPONSIBILITY FOR CYBER ATTACKS: COMPETING STANDARDS FOR A GROWING PROBLEM. Conference on Cyber Conflict Proceedings 2010: CCD COE Publications, 2010, Tallinn, Estonia. https://ccdcoe.org/uploads/2018/10/Shackelford-State-Responsibility-for-Cyber-Attacks-Competing-Standards-for-a-Growing-Problem.pdf

as well as any other state to ensure respect for IHL. According to the Article 90 of Protocol I which establishes a Fact-Finding Commission the targeted state should compensate the injured state according to the IL as well as their victims. In case where the cyber conflict was occurred as part of an internal conflict, then the state should be responsible of the nationals as part of their concern. In the event where the targeted state did not take any countermeasure then the injured state has the right to take steps against the other state as part of its obligation. However, if a reprisal occurred towards civilians or civilian objects it should be prohibited as an opposite[175] act cannot include another wrongful act that could trigger the violation of IHL rules.

Also, in its 3rd Article, the ILC Draft also stipulates the idea of an act that may be attributed to a state when the act itself is conducted by a representative of a state organ or an individual that acts on behalf of a state. This would intrigue the responsibility that a state should held in case of cyber attacks made by its own consent, however, sometimes state may waive the international responsibility for particular foreseen reasons and these are mentioned in the Chapter V of the ILC Draft which include reasons such as the consent validly given by a state (article 29), countermeasures in respect of an internationally wrongful act (article 30), force major and fortuitous event (article 31), extreme distress, required by the purpose of saving human life (article 32), state of necessity (article 33) and self-defence, in accordance with Article 51 UNC (article 34).

Consequently, if the state should be attributed the attack and establishes an international responsibility it needs to show how the act has violated a specific international law rule and contribute and analyses of the act that had violated or created

[175]State responsibility | How does law protect in war? - Online casebook. (n.d.). https://casebook.icrc.org/glossary/state-responsibility

an issue to another particular state. And, even if Article 2 of the UN Charter prohibits the use of force in international relation, a cyber attack conducted by a state towards another state may be seen as another way of use of coercive method which therefore would constitute a breach of international law anyways. It's true that a cyber attack can be difficult to determine its physical location and the person behind the computer, however, it is not consider that extremely difficult, the only difficulty is the localization of the physical computer not the localization in general.

In addition, a state should be responsible to take all reasonable and necessary actions and measures to prevent an act of cyber mean. Even, if the state is not warrant of such an event that may occur, it also should take responsibility by taking measures of any means as well as taking responsibility of quasi-legal persons. For example, in the Estonia attacks which was held by the Naszi organization, the government did not take any measures and did not prevent them, in this case the attacked state is responsible for any act that violates its sovereignty and it has the obligation to conduct and initiate an international debate on the applicability of responsibility principles since the cyber attack could threat it's peace and security as well as the international one.

Overall, states should have the responsibility to attribute the cyber attacks to their own state when engaging or starting in a cyber conflict, as well as achieve cyber deterrence. States should warn other parties about cyber attacks before even engaging in one and they should be responsible for attacks that are under the control of non-state actors. National governments should stop third party attacks also as a part of their state responsibility unless the state is unable to stop the third party attack or in unwilling to take any official action. It is important that a state encourages to control cyber attacks from non state actor or third party controls as a matter of their governance policy or

coordinates with them so that the attack is under the responsibility of the state. Cyber attacks should be a well matter of study and discussion between states and their national government.

4.5 Regional and international cyber security.

Cyber attacks and conducted by using a computer and the Internet which tries to steal key information structures of another state just like the attack on Estonia or the many attacks that U.S electronic infrastructure had seen which were attributed to other governments, or individuals because of the danger and gravity that these attack held and the arise of a cyber warfare situation. Since we become a world where technology is dominated, it is important to secure a state and have technological safety. As the EU has declared in its 2010 agenda, the issue of cyber security is indeed important and it is essential to legally permit states to self defence in case of a cyber attack. Many governments have declared very important declarations regarded cyber attacks, for example Russia had expressed several times that it feel authorized to use nuclear in response to cyber attacks. The Clinton and Bush administration had also enhanced the difference between cyber weapons and traditional ones as a major threat.

According to the Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations an intervention whether external or internal is considered a breach under IL. It has expressed that any type of intervention whether involves arms or not it is still considered an illegal form of intervention because it has an element of threat. Also, according to Article 32 of the Charter of Economic Rights and Duties of States[176] it

[176] According to the Charter, every state has to right to engage in international trading and economic operations regardless of their political, economic and social sytem.

stipulates that a state cannot use any economic, political or other type of measure to coerce another state and by saying any other measure it involves technology too.[177]

It is important to note that states should take measures by enhancing cyber security programs to prevent any cyber attack against the state. Any state has the responsibility to be ready if a cyber attack occurs which can violate the sovereignty of the state and put its civilian in danger. This responsibility comes individually for states as well as regional. For example, the ASEAN [178]organization has expressed its interest in progressing with its cyber security programs to secure its economic progress as well since we are living nowadays in a digital world where economy is also part of it. After the COVID-19 crisis, the world also adopted a rapid digitization as well as the idea of a government migration and online business. As a result, many cyber attacks occurred within that period of time which had an impact in the real world. Therefore, the ASEAN group for example made an strategy by implementing *Confidence Building Measures (CBMs)*, which is an important initiative that could prevent future cyber attacks and make cyberspace in the region more safer. [179]

In addition, other regional organizations like the NATO, have also implemented a cyber defense strategy, as they have affirmed that IL applies to cyberspace. Their main focus is to protect their networks from cyber attack by it's Alliance's cooperation and missions. They have created platforms for political consultation and a collective action

---

[177] Vakulyk, O. (2020). https://www.researchgate.net/publication/340440328_CYBERSECURITY_AS_A_COMPONENT_OF_THE_NATIONAL_SECURITY_OF_THE_STATE. Journal of Security and Sustainability Issues 9(3):775-784. https://www.researchgate.net/publication/340440328_CYBERSECURITY_AS_A_COMPONENT_OF_THE_NATIONAL_SECURITY_OF_THE_STATE

[178] The Association of Southeast Asian Nations (ASEAN) is a regional organization that was created in 1967 and includes 10 member states. (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar (Burma), the Philippines, Singapore, Thailand and Vietnam.) The organisation objective is to establish a cooperation in the economic, social, cultural, technical, educational and other fields, and to promote regional peace and stability through abiding respect for justice and the rule of law and adherence to the principles of the United Nations Charter.

[179] ASEAN CYBERSECURITY COOPERATION STRATEGY. (2021). ASEAN Organization. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

plan. For example, in 2016 they recognized cyberspace as a domain in which NATO should defend as they do in air, land or sea. They have reinforced their strategies by including training and exercises and well as sharing mutual assistance to prevent cyberattacks and recovering from them. They also created a cyber rapid reaction team that works 24 a day. In 2018, they set up a Cyberspace Operations Centre as part of NATO's strengthened Command Structure which provides situational awareness and coordinates NATO's operational activity in and through cyberspace. Both NATO and the EU they cooperate through a Technical Arrangement on Cyber Defence, which was signed in February 2016. The agreement tries to facilitate technical information sharing between NCIRC and CERT-EU[180] to improve cyber incident prevention, detection and response in both organizations, in line with their decision making autonomy and procedures. NATO's main aim on cyberspace is to promote a free, peaceful and secure environment in which it can reduce the risks of a cyber conflict by supporting IL and the norms of a state's responsibility and behavior in cyberspace.

Also, the EU had stepped in advancing through cyberspaces capabilities, in 2020 they opened a discussion in where they provided a safe and secure cyberspace environment through quantum encryption and judicial and law enforcement for data access purposes. In the same year, they have also presented a cybersecurity strategy through the European Commission and the European External Action Service (EEAS) which aimed to strengthen its resilience to cyber threats. In 2021, the council adopted another strategy which aimed to build a resilient, green and digital Europe. In 2019, the EU began adopting a cybersecurity act which became an important act for cyber security matters in the region which latter on made them do a single EU-wide certification framework which makes cybersecurity grow by building trust and

[180] The Computer Emergency Response Team for the EU institutions, bodies and agencies.

enhancing easy trade. They have also established a EU Agency for Cybersecurity that deals with cyberattacks.

Another example can be set through the African Union (AU) which was established in 2000 and consists of 55 African states to make peace and form security in the region as well as established socioeconomic developments in the continent. It has been viewed that cybercrimes and cybersecurity is a well concerned topic in the region. They have established an African Union Convention on Cyber Security and Personal Data Protection in 2011 to form a cybersecurity framework which gives personal data protection and combats cybercrimes. The convention was finally adopted in 2014 after many postulations. However, the only problem about the convention is that only 5 members have ratified and only 14 have signed. The AU also cooperates with the Council of Europe Cybercrime Programme Office (C-PROC) via the latter's Global Action on Cybercrime Extended (GLACY+) project which aims to strengthen the ability and capacities of states to apply legislation on cybercrimes and try to create an effective international cooperation. The AU convention on cybersecurity highlights the importance of having cyber security by adhering to national constitutions and IHRL. For example, in its article 24 of the convention it states that each party should develop a national cyber security policy as well as other provisions that outlines the measures that should be taken to protect citizens personal data and the responsibilities that a state should take regards measures and cyber security safety.

Moreover, the League of Arab States (LAS) on Cyber security has also been in development. The league was was established in 1945 and it compromises 22 member states. The region has been adopting several cybercrime measures to improve the quality of cybersecurity in the region. In 2006, United Arabic Emirates (UAE) was the

first Arabic country that adopted a cyber legislation called Cyber-Crime Law no 2 which focuses on a new conduct for violating the orivacy of others such as criminalizing eavesdropping and other cyber malicious acts, along with other countries that had also adopted cybercrime legislation like Pakistan and Saudi Arabia. In 2007, the Gulf Cooperation Council (GCC) which involves several Arab countries like Bahrain, Oman, Kuwait, Saudi Arabia, Qatar and the UAE held a conference where they suggested to make a cyber crime treaty. Following the next year in 2008, workshops in Doha were held regarding an ITU Regional Workshop for Cybersecurity and Critical Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop which highlighted the importance on having a national cybercrime legislation to combat cyber crimes. Also, in 2010, the first regional IPR and Cybercrime Conference was held in Jordan which also discussed the idea of making new laws of cybercrime in the Arab region and protect the user and the private cyber industry and in the same year they have adopted an Arab Convention on Combating Technology Offences which combats cyber attacks and crimes and protects the security of cyberspace in the region.

Additionally, the Organization of American States (OAS) is also an important and effective regional organization that compromises of 35 states in the American continent. The OAS has a major interest in the cyberspace field specially the cybersecurity stability in the region and strengthening its capacity. It has created the Inter Americana Committee on counter-terrorism (CICTE) which aids to developing the cybersecurity in Latin American States and prevent and combat terrorism in the region. The OAS cyber policy is based on a comprehensive Inter-American Strategy to Combat Threats to Cybersecurity as well as establishing a National CSIRT[181], strengthening Hemispheric

[181] A computer emergency response team (CSIRT) with National Responsibility (or "National CSIRT") is a CSIRT that is designated by a country or economy to have specific responsibilities in cyber protection for the country or

Cooperation and Development in Cybersecurity and Fighting Terrorism in The Americas, protecting the region from critical infrastructures from emerging threats, such as cyber-terrorism. They also held meetings on cyber crime and building measures, in addition to implementing agencies and committees like the Inter-American Committee against Terrorism (CICTE) that tries to prevent and defeat terrorism and the Inter-American Telecommunication Commission (CITEL) that aims to facilitate and promote the integral and sustainable development of interoperable, innovative and reliable telecommunications in the region based on universality, equity and affordability.

4.6 National and local laws of powerful states on Cyber-attacks.

Cyber crimes are considered a red cross limit around the world because of its danger on the national security level and the international level too which may cause tensions between states. The cyber crime domain is concerns every state and affects both the governments and the people. 80 % of states worldwide have cyber crime legislation which counts approximately 156 states. Europe itself has the highest adoption rate with a 91% and Africa which comes the lowest with 72%. Cyber crimes have become a challenging issue for law enforcement that states are forcing their national cyber security.

The cyber law domain has become an important part of the internet security system because it regulates any law that involves the use of computers. As technology keeps changing, the laws that governs digital communication also changes which makes sense to keep developing cyber laws in each state. Cyber law is very important because it protects victims from cyber crimes and it also creates rules and limitations for those

economy. A National CSIRT can be inside or outside of government, but must be specifically recognized by the government as having responsibility in the country or economy.

who use the internet. It monitors activities related to fraud, copyright, defamation, online harassment, freedom of speech and business related topics like trading. In this section it will be discussed different types of local law for powerful states and regions to kind of present how can a state protect a persons internet life and how each law is being regulated. It will be only given two examples to clarify the idea more about how powerful states work in relation to cyber attacks and cyber security.

4.6.1 The U.S

The United States is one of the countries that has a big interest in the cyber field. The U.S has 3 types of cyber regulations. The Federal Government Regulation, Federal Laws and State Laws. The Federal Government Regulation has three main cybersecurity regulations which include, the 1996 Health Insurance Portability and Accountability Act (HIPAA)[182], the - 1999 Gramm-Leach-Bliley Act [183] and the 2002 Homeland Security Act[184] which includes the Federal Information Security Management Act (FISMA)[185]. These three regulations are responsible for healthcare and financial institutions cyber security as well as federal agencies to ensure the protection of their computers system and information.

However, many critiques have been address regarding these regulations noting the

[182] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a U.S federal law that creates national rules to protect the information a health's patient from being exposed without his consent or knowledge.
[183] The Gramm-Leach-Bliley Act of 1999 (GLBA) was a bi-partisan regulation under President Bill Clinton, passed by Congress on November 12, 1999. The GLBA prupose is to modernize the financial industry and it was known as the repeal of the Glass-Steagall Act of 1933, which stated that commercial banks were not allowed to offer financial services—like investments and insurance-related services as part of normal operations.
[184] The Homeland Security Act is a U.S. legislation signed into law by President George W. Bush on November 25, 2002, that established the Department of Homeland Security (DHS) as a new department in the executive branch of the government that aimed at protecting the national security of the United States.
[185] The Federal Information Security Modernization Act of 2014 (FISMA 2014) is an act that updates the Federal Government's cybersecurity practices by implementing new rules such as codifying Department of Homeland Security (DHS) authority to administer the implementation of information security policies for non-national security federal Executive Branch systems, including providing technical assistance and deploying technologies to such systems.

fact that the rules are not quite considered a bulletproof for attacks and that to secure the date there has to be reasonable level of security. Further, these regulations do not address all the computer related industries like the Internet Service Providers (ISPs)[186] and software companies. Furthermore, discusses about the how companies will not try to invest as much as they should in cybersecurity unless the government compels them to do so.

Moreover, the U.S has other Federal Laws regarding the cyber security laws which includes the Cybersecurity Information Sharing Act (CISA)[187] which enhances the security of the state from cyber threats. The Cybersecurity Enhancement Act of 2014 which improves the cybersecurity and enhances researches and development. The Federal Exchange Data Breach Notification Act of 2015 and finally, the National Cybersecurity Protection Advancement Act of 2015 which takes measures to improve cyber security. The U.S has also its main act regarding cyber crimes called the *"Computer Fraud & Abuse Act"* which regulates law regarding cyber crimes that could be the result of an internet abuse or computer fraud.

4.6.2 China

China's is one of the countries that keeps developing in the technological field. Since it faces many cybercrime issues, the country itself had created law and regulations that could improve the cybersecurity of the state. China has two main organizations that responsible for internal and external security of the state, the Public Security Bureau

[186] (internet service provider) is a company that provides individuals and organizations access to the internet and other related services.
[187] The act is responsible to notify each individual whose personal information is known to have been acquired or accessed as a result of a breach of security of any system maintained by the exchange as soon as possible but not later than 60 days after discovery of the breach.

(PSB), which is responsibly for the internal security, and the Ministry State Security (MSS), which takes care of the external security. The PSB is codified in the *"Computer Information Network and Internet Security, Protection and Management Regulations"*. One of the main institutions of law in china since 1996 that relates to technology is the Ministry of Information Industry (Department of Policies, Laws and Regulations).

China has one of the most amazing and interesting applicable laws regarding technology. They have the Cybersecurity Law which entered into force in 2017 and it covers a variety of aspects including network security. The country has been developing measures to facilitate the implementation of the Cybersecurity Law such as the Measures for Cybersecurity Review, the National Emergency Response Plan for Cybersecurity incidents and finally the Provisions on Protection of Children's Personal Information Online. China's Cybersecurity Law protects the network security of Chin and its designed to improve a graded protection.

In 2021, China had also created a Data Security Law which helps to provide security measures to protect data. Further, it has also created the Personal Information Protection Law in the same year which protects the personal data and information of each user. A year before, China had also implemented the Cryptography Law and manages regulations for cryptography.[188] Under the China's Criminal law which came into force in 1997 and is considered the most important cybercrime law in china states in its Article 285 that those who violate the cyberspace and engages with information

[188] Global Legal Group. (n.d.). Cybersecurity Laws and Regulations Report 2022 China. International Comparative Legal Guides International Business Reports. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/china

that concerns the state it can be sentences up to three years. [189]

By that means, its important to note that China digitization has become an important matter and a way of force to grow the economic aspect and create new opportunities for Chinese companies globally. The digital economy has become an essential business to operate, which means that the country has to always develop and reinforce the cybersecurity legislation to protect the security and date of the country. China is known for its Going Out Policy and Open Door Policy which means that it has to reinforce the digital domain and create new measures for data control and intellectual property protection. For instance, Beijing the capital of China had process the Cybersecurity Multi-Level Protection Scheme (CMLPS 2.0) to protect the cybersecurity of the Chinese people in terms of data protection, trade secrets and business information.

4.6.3 Russia

Russia is a very interesting example on a new context for cyber security and laws. It is known that Russia is very interested in cyber operation and it was seen specially in the latest Russian-Ukrainian war were Russia had threaten NATO to use nuclear weapons through cyber means. Russia is a world powerful state in which has local data protection like the Federal Law No. 152-FZ[190] dated 27 July 2006 “On Personal Data” (the “Data Protection Law”) and the Labour Code of the Russian Federation (for

[189] Yong, P. (n.d.). Comparative research on “ Convention on Cybercrime” and Chinese relevant legislation. https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567%20china-d-Comparative%20Research_ed1a.PDF

[190] This Federal Law regulates the relationships relating to the processing of personal data by federal governmental bodies, governmental bodies of subjects of the Russian Federation and other governmental bodies, local self-government bodies and other municipal bodies , legal entities and natural persons by means of automation facilities, for instance in information-telecommunication networks, or without such facilities, if the processing of personal data without the use of such facilities corresponds to the character of the actions (operations) as involving the personal data by means of automation facilities, i.e., allows to search - according to a set algorithm - for the personal data recorded on a material medium and available in card files or other systematised corpuses of personal data and/or access to such personal data.

personal data of employees[191]). Russia had also implemented a data protection authority like the Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Minkomsvyaz) and the Federal Service for Supervision in the Sphere of Telecom, Information Technology and Mass Communications (Roskomnadzor). Russia had many anticipated changes to local law. For example, it has signed the Amending Protocol updating the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.[192] For example, Russia had suggested to introduce a new breach notification obligation a a new category for sensitive personal data.

In addition, Russia has a different concept for cyber operations. It does not use the term cybersecurity but rather information security. Also, it uses the term information weapons rather than cyber weapons. Russia includes more than just digital measures, it defines information technology as the means and methods that are used in a waging information war. These methods include, the spreading of disinformation, electronic warfare, the degradation of navigation support, psychological pressure, and the destruction of adversary computer capabilities.

In 2019, Russia had adopted a new cyber law which refers to Russia's sovereign internet which allows the government to disconnect from the global internet. Russia's views on cyberspace is connected to the domestic information space which is essential to the security of the state and a main element to the state sovereignty. This is why, Russia had recently implement the digital sovereignty concept in which it secures the domestic information space of the country. The concept is political and it is related to

[191] The purposes of the labor law is to guarantee labor rights and freedoms of the nationals, creating favorable conditions for work, protecting rights and interests of employees and employers.
[192] .The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) The Convention opened for signature on 28 January 1981 and was the first legally binding international instrument in the data protection field.

the right and capability of the government to determinate the fate of the state through the information space. Russia had developed the concept of digital sovereignty to a electronic sovereignty which is the internet infrastructure system and its protection from cyber malwares and attack.second, the information sovereignty which is the control over the information and data. [193]

In 2012, Russia had launched the Internet Blacklist law which monitors the sphere of Telecommunications, Information Technologies and Mass Communications as well as the Foreign Agents Law. In 2014, Russia had also implemented more digital laws like the Law on Bloggers,Law on data localization, Law on phone number provision for Wi-Fi, government decree. In 2016, it had launched the Yarovaya' package of laws,which requires ITC providers to store content and related metadata, and disclose them to authorities without court order and in 2019 it had implemented the Sovereign Internet law which is the most interested one in which we have discussed above. [194]

4.6.4 EU

The European Union (EU) had many impacts on cybersecurity and had been overdeveloping their foreign and national cybersecurity policy. They had a great impact in organizations, companies and institutions worldwide and they have been improving in their cybersecurity and cyber laws. The EU had introduced a wide cybersecurity framework like the ENISA ('European Union Agency for Cybersecurity') which provides support to EU member states, businesses, and institutions in the cybersecurity sector and delivers solutions and improvements to the EU's cybersecurity framework.

[193] Hakala, J., & Melnychuk, J. (2021). RUSSIA'S STRATEGY IN CYBERSPACE. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf

[194] IBID,134

they have also implemented the EE (European Energy) - Information Sharing and Analysis Centers (ISACs) which aids in thwarting cyber threats. Also, the European Cyber Security Organization (ECSO) which was established in 2016 and represents the industry-led contractual counterpart of the European commission on implementing the cyber security of the region that rovides all initiatives to develop, promote and protect the European cybersecurity, the Computer Security Incident Response Teams (‘CSIRTs’) and the Computer Emergency Response (or ‘Readiness’) Teams (‘CERTs’) which deals with cybersecurity incidents on the spot.

The EU had many efforts in implementing rules and measures on cybersecurity. For example, in 2011 they have a direct effort on combating the sexual exploitation of children online and child pornography. in 2013, they had a directive aim on attacks against information systems and they had strengthen the national cyber crime law by introducing cyber crime sanctions. In 2018, they had a proposal for Regulation and Directive facilitating cross-border access to electronic evidence for criminal investigations and in 2019 they had updated their legal framework on fraud and counterfeiting by implementing a non-cash payment. In 2020, they had a proposal for an interim Regulation on the processing of personal and other data for the purpose of combatting child sexual abuse.[195]

[195] The EU Cybersecurity Act. (2022, November 28). Shaping Europe’s Digital Future. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Chapter 5: Conclusion and Recommendations.

International law is an important legal source to deal with international problems and in maintaining stability and order in the international system. When it comes to cyberspace, IL also offers security and stability when conducting rules to states which is recognized by the international community. According to a recent Open-Ended Working Group (OEWG) report in 2021, which was introduced through the resolution 73/27 by the General Assembly in which all UN Member States are invited to participate. The OEWG is considered important since it provides the possibility of holding intersession consultative meetings with industry, non-governmental organizations and academia.

During the OEWG latest report, it had concluded and reaffirmed that IL and specially the UN Charter applies to cyberspace by ensuring peace and stability while accessing ICT information and secure and open and peaceful cyber environment. This thesis was to bring out the purpose of the current study which was to determine how cyber attacks are dealt with in international law and if they are considered legal or unlawful. The main aim of the study was to examine different topics in international law like the principle of sovereignty, non-intervention, international humanitarian law and other subjects and how are they applied in cyberspace and cyber attacks.

Multiple regression analysis about cyber attacks in international law have revealed several points are the results of this thesis and an answer to our main question which is how IL is applicable to cross border cyber attacks by analyzing its norms and principles?. How can the conduct of cyber attacks and warfares lead to a serious breach under IL and IHL?

Results:

First, in accordance with the UN Charter, Article 2(4) is the main core when dealing with cyber attacks since the rule prohibits the use of force or threat to any territorial of a state or political independence. Depending on the facts and circumstances, conducts by states using cyberspace cannot include threat or use of force that could have the same effect as using kinetic means.

Second, either kinetic or cyber means, if an effect is similar by the end of the attack, this is considered a breach under IL. An operation that is carried out by a cyber mean can be considered an armed attack since the effect can lead for the individual to use self defence as it is recognized by the Article 51 of the UN Charter where the effects scales to the point where they are equivalent to kinetic attacks which include physical

destruction of property, or injury of an individual and even death. Using kinetic or cyber means must always fulfill the requirements of necessity and proportionality.

Third, Article 2(3) and the provisions of Chapter VI of the Charter on the peaceful settlement of disputes can also apply to states conduct and activity in cyberspace. Thus, conforming to Article 33(1) of the same provision, states that are part of any cyber related international dispute which can lead to an instability and danger of international peace and security, should endeavour to settle such dispute as it is described in the article 33 of the Charter on the peaceful settlement of disputes which include negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice.

Fourth, the threat or use of force also is dictated in the customary international law rule which prohibits intervention into domestic affairs of another state and this includes cyber operations just like any other kinetic activity. As set out by the ICJ in the Nicaragua case, the purpose of non-intervention is to ensure that states refrain from using coercive means which affects the state power and can violate the sovereignty and freedom of the state.

Fifth, a state is responsible of cyber activities under IL, in particular those that are attributed to the state. The state is responsible for any activity in cyberspace as determined by the international law rules on state responsibility. Also, the state is responsible of its agents and organs, meaning that if an individual or a collective group of people acts on behalf of the states instructions or under its direction and control, then the state takes responsibility.

Sixth, Norm 13 (c) of UNGGE provides that states should not allow their territory to be used for internationally wrongful acts including using information and communications by technology. This norm provides a guidance on what a state behaviour should be.

Seventh, states should always apply countermeasures against any state that participates in cyber activities that constitute an international wrongful act. If a state in injured by a cyber operation, then the injured state must take countermeasures against the state which was originally responsible for the international wrongful act in order to make the state to comply with it's obligations. The measures taken by the responsible state must indeed be commensurate with the injured state and it should be in accordance with the restrictions and conditions carried out by the IL rules and it should not imply any threat or use of force.

Eighth, when it comes to human rights law, a state must follow its human rights obligations in activities that are related to cyberspace just like any other activity. States must follow the rules and norms set by international law and protect the rights of individuals when using technology just like it is affirmed by the Human Rights Council Resolution 20/8 which affirms that individuals should be protected when online and offline and states should have the obligation to act in accordance with international human rights law, including customary international law and international treaties and conventions which they are party to like the International Covenant on Civil and Political Rights or UN treaties as well as regional conventions like the European Convention on Human Rights. Hence, states must ensure a safe, open and stable access to the technological environment for individuals and ensure to not permit an unlawful interference that could violate their privacy.

Ninth, states must also comply with International Humanitarian Law norms when dealing with cyberspace since IHL applies to cyber operations which are conducted by hostilities in an armed conflict just like military operations. Since IHL protects those who are not or no longer participating in a hostility and it limits the means and methods of warfare by belligerents, it also protects them in cyber operations specially those that are used as part of a militarization mean by cyberspace.

Finally, according to IHL and by analyzing the UN Charter, a cyber attack can have the same effect of a kinetic attack which would constitute a cyber warfare since the attack can integer the principles of proportionality, necessity, distinction and military to be applied just like any non cyber attack. Under IHL civilians are protected from the attack unless they take part of the hostility they loose their protected. So in a cyber attack civilians must be protected as well as their objects and those who are responsible of planning and executing the cyber attack should be attributed responsible whether the cyber operation was complex or simple.

In the final analysis, the findings of this research provide insights for international law which is applicable to states activities in cyberspace with the presence of the UN Charter, customary international law and regional instruments and unless there is no rule that applies to a certain situation by a cyber attack then opinio juris is invoked to indicate which rule is applicable. These findings contribute in several ways to our understanding of cyber attacks and provide a basis for all principles of international law which apply to cyber operations just like any other international wrongful act specially the principle of sovereignty. A remote act carried by a state against another with or without consent of the harmful effects may be a violation of sovereignty. On the other hand, when it comes to the scale and degree of the effect by a cyber activity there is not

much enough state practice or opinio juris to say how it is reflected in customary international law. The coercive practice that is carried out by a state or a non-state actor is attributed to the state under the rules of state responsibility whether it was direct or indirect, overt or covert. If the cyber attack constitutes of a malicious behavior that pressures the targeted to state to be deprived from its free will then the non intervention principle is applied unless the cyber act did not have coercion means. In due course, state must follow the norms of IL and need to make informed decisions to where their own position lies on the application of IL to cyber attacks.

The scope of this study was limited in terms of finding an international treaty that deals with all principles of international law and international humanitarian law and how they are applied in cyber attacks. Also, there were not many cases to rely on that could be an attribution and help to the study, most of the analysis was based on theoretical information which somehow limits the study and makes it more efficacious. In spite of it's limitations, the study certainly adds to our understanding of cyber attacks and operations and how are they understood in international law and this is thanks to the Tallinn Manual which is of a big contribution and a possible new international treaty in the future. All of our research questions were answered which is a successful study despite of the limitations and this study could be a main reference when studying cyber attacks in international law as well as a future research that could be more developed in other areas of international law specially since there are remained questions not answered like the legality of cyber nuclear weapons in international law.

Recommendations:

Firstly, states must let their intelligence agencies and their foreign services to gather together and be united and decide on their legal position and indicate when there is an beach of obligation.

Then, states must make open forum discussions if they disagree on how the law applies to a certain cyber activity and discuss issues in more open way and involve not just states but academic, private sector organizations and the civil society to discuss the issues of cyber attacks.

More importantly, state need to work more on the Tallinn Manual 2.0 and other initiatives and discuss the principles of sovereignty and non-intervention in cyber context and take into consideration past UNGGEs.

Besides, there must be a general treaty that deals with cyber attacks and every state should be part of it or make the Tallinn Manual an international treaty adopted by the UN.

Also, states should create a national cyber security strategy by developing their cyber security policy, conduct a security risk assessment and conduct phishing campaigns for employees and implant a security awareness training.

Further, states should developed national cybersecurity centers and programs, and implement a trusted internet connection initiative that reduces potential cyber threats to government networks and limits internet trafficking and create intergovernmental partnerships.

Furthermore, states need to create a cybersecurity workforce development center to build a cybersecurity team from professionals that could secure the nation’s digital asset and protect against cyber threats as well as the cyber military security system and it’s

infrastructure system to ensure more effective missions and less collateral damages to civilians.

Moreover, states also need to adopt new national strategy policies for trusted identity in cyberspace to support the protection of privacy and civil liberties to minimize cyber attacks to civilians.

Finally, it’s essential to look at further visions and focus on how international law can be applied to state-sponsored cyber operations. If the act is considered a wrongful international act or not and if there is more commonality about how it applies the law on this specific act.

Bibliography.

Websites and E-books

Ahmed, S. G. (2018, December 15). Cyberwarfare and the Applicability of the Principle of Distinction. *Available at SSRN.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301834

Aravindakshan, S. (2021). Cyberattacks: a look at evidentiary thresholds in International Law. *Indian Journal of International Law (2021) 59(1–4):285–299.* https://link.springer.com/content/pdf/10.1007/s40901-020-00113-0.pdf

Bannelier, K. (2017, February 25). Cyber-Attacks Prevention-Reactions: The Role of States and Private Actors. Available at SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

Bern. (2009). ABC of International Law. *Swiss Federal Department of Foreign Affairs (FDFA)*. https://www.eda.admin.ch

Beson, S. (2011). *Sovereignty*. Oxford Public International Law. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472

Brown, G., & Poellet, K. (2012). *The Customary International Law of Cyberspace*. Strategic Studies Quarterly, 6(3), 126–145. http://www.jstor.org/stable/26267265

Bussolati, Nicolò, 'The Rise of Non-State Actors in Cyberwarfare' (January 1, 2015). In: Jens David Ohlin, Kevin Govern, and Clair Finkelstein (eds), Cyber War: Law and Ethics for Virtual Conflicts, (Oxford University Press, 2015) p. 102-126., Available at SSRN: https://ssrn.com/abstract=2764185

Butchard, P. (2020, September 21). *Principles of international law: a brief guide*. House of Commons Library. https://researchbriefings.files.parliament.uk/documents/CBP-

9010/CBP-9010.pdf

Cohen, K. (2020). *Introduction History of Technology*. San José State University. https://www.sjsu.edu/people/patricia.backer/history/introduction.htm

Coman, I. M. (2017). *Cross-Border Cyber-Attacks and Critical Infrastructure Protection*. Mendeley. https://www.mendeley.com/catalogue/828ef704-37f5-36be-83ff-6fd530c640fe/

Common cyber attacks: reducing the impact. (2016). National Cyber Security Centre. https://www.ncsc.gov.uk

Comprehensive Study on Cybercrime. (2013). UNITED NATIONS OFFICE ON DRUGS AND CRIME. https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

Council of Europe. *Cybercrime Convention Committee*. Cybercrime. https://www.coe.int/en/web/cybercrime/tcy

Cybercrime Legislation Worldwide. UNCTAD. https://unctad.org/page/cybercrime-legislation-worldwide

Cybercrimes. United Nations : Office on Drugs and Crime. https://www.unodc.org/unodc/en/cybercrime/index.html

Cyberwarfare and international humanitarian law: the ICRC's position. (2013). ICRC. https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf

Doctors without borders | The Practical Guide to Humanitarian Law. https://guide-humanitarian-law.org/content/article/3/proportionality/

Donovan, D., & Robert, A. (2006). *NOTES AND COMMENTS THE EMERGING RECOGNITION OF UNIVERSAL CIVIL JURISDICTION*. Law Yale. https://documents.law.yale.edu/sites/default/files/Donovan100AmJIntlL142[1].pdf

F. Sinopoli, A. (2012). *Cyberwar and International Law: An English School Perspective*. University of South Florida Scholar Commons. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=5600&context=etd

Gardam, J. G. (1993). *Proportionality and Force in International Law*. The American Journal of International Law, 87(3), 391–413. https://doi.org/10.2307/2203645

Geers, K. (2008). *Cyberspace and the Changing Nature of Warfare*. Hakin9 E-Book, 19(3) No. 6; SC Magazine (1-12). https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf

GIOVANNELLI, D. (n.d.). *Proposal of United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes: Comment on the first draft text of the Convention*. CCDCOE. https://ccdcoe.org/library/publications/proposal-of-united-nations-convention-on-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes-comment-on-the-first-draft-text-of-the-convention/

Gisel, L. (2016). *THE PRINCIPLE OF PROPORTIONALITY IN THE RULES GOVERNING THE CONDUCT OF HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW*. INTERNATIONAL EXPERT MEETING. https://www.icrc.org/en/document/international-expert-meeting-report-principle-proportionality#:~:text=The%20principle%20of%20proportionality%20prohibits,and%20direct%20military%20advantage%20anticipated.

Global Legal Group. (n.d.). *Cybersecurity Laws and Regulations Report 2022 China*. International Comparative Legal Guides International Business Reports. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/china

Gupta, B. B., A.G. Arachchilage, N., & E. Psannis, K. (2017). *Defending against*

Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions. https://arxiv.org/ftp/arxiv/papers/1705/1705.09819.pdf

H. Hook, D., M. Norman, J., & R. Williams, M. (2002). *ORIGINS OF CYBERSPACE A Library on the History of Computing, Networking, and Telecommunications*. History of Science. https://www.historyofscience.com/pdf/cyberspace-prospectus.pdf

Hanel, A. (2022, March 18). *Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware*. crowdstrike.com. https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

Hathaway, O. (2011). *The Law of Cyber-Attack*. Research Gate. https://www.researchgate.net/publication/251334352_The_Law_of_Cyber-Attack

Heselhaus, S. (2014). *INTERNATIONAL LAW AND THE USE OF FORCE*. Encyclopedia of Life Support Systems (EOLSS). https://www.eolss.net/sample-chapters/c14/E1-36-01-02.pdf

Higson, D. (2016). *Applying the Law of Neutrality While Transitioning the Seas of Cyberspace*. University National Security Law Brief, Vol. 6, No. 2 (2016). https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1102&context=nslb

International cyber law: interactive toolkit. (2022, September 12). *Self-defence*. International Cyber Law: Interactive Toolkit. https://cyberlaw.ccdcoe.org/wiki/Self-defence.

International cyber law: interactive toolkit. (2022a, September 12). *Due diligence*. International Cyber Law: Interactive Toolkit. https://cyberlaw.ccdcoe.org/wiki/Due_diligence

Khan, A. (2017, November 3). *Cyber Attacks in International Law: From Atomic War to Computer War*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064787

Komljenović, A. (2018). *Espionage and its Relation to Diplomats and Intelligence Officers*. European Perspectives − International Scientific Journal on European Perspectives Volume 9, Number 1 (16), Pp 37-64, October 2018. https://www.europeanperspectives.org/storage/71/04-International-Scientific-Journal-on-European-Perspectives-Maj-2019-internetAljosa-Komljenovici.pdf

Lee, W. (2019). *Malware and Attack Technologies Knowledge Area Issue 1.0*. https://www.cybok.org/media/downloads/Malware__Attack_Technology_issue_1.0.pdf

Liab, Y., & Liu, Q. (2021). *A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments*. Energy Reports Volume 7, November 2021, Pages 8176-8186. https://www.sciencedirect.com/science/article/pii/S2352484721007289#:~:text=Cyber%20attack,asset%20is%20called%20cyber%2Dattack.

Liivoja, R. (2015a). *Technological change and the evolution of the law of war*. International Review of the Red Cross (2015), 97 (900), 1157–1177. https://www.corteidh.or.cr/tablas/r35988.pdf

Lotrionte, C. (2012b). *Cyber Operations: Conflict Under International Law*. Georgetown Journal of International Affairs, 15–24. http://www.jstor.org/stable/43134334

Madubuike-Ekwe, J. N. (2021, April 8). *Cyberattack and the Use of Force in International Law*. https://www.scirp.org/journal/paperinformation.aspx?paperid=109997

Mallick. M, (2021). *Cyber weapons; a weapon of war?* Vivekananda International Foundation. Found at: https://indianstrategicknowledgeonline.com/web/Cyber-Weapons-A-Weapon-of-War.pdf

Margulies, P. (2015a, January 29). *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2557517

Michael, N. (2013). *Tallinn manual on the international law applicable to cyber warfare : prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. NATO Cooperative Cyber Defence Centre of Excellence. https://wrlc-gulaw.primo.exlibrisgroup.com/discovery/fulldisplay?docid=alma991007869929704113&context=L&vid=01WRLC_GUNIVLAW:01WRLC_GUNIVLAW&search_scope=MyInst_and_CI&tab=Everything&lang=en

Moscow, I. (2018, February 16). *Cyberspace operations in armed conflicts and the proportionality rule*. Humanitarian Law & Policy Blog. https://blogs.icrc.org/law-and-policy/2016/06/29/cyberspace-operations-armed-conflicts-proportionality-rule/

Moulin, T. (2020, July 31). *Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward*. Journal of Conflict and Security Law, Volume 25, Issue 3, Winter 2020, Pages 423–447. https://academic.oup.com/jcsl/article/25/3/423/5879500

Moynihan, H. (2019). *The Application of International Law to State Cyberattacks Sovereignty and Non-intervention*. Chatham House, International Law Programme. https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf

Mozid, A. (2020). *Term Paper on The Nature of Cyber Crime and Cyber Threats: A Criminological Review*. Mendeley. https://www.mendeley.com/catalogue/e2bce7c7-1f98-3e09-a02d-7d52672ed886/

Mschneer. (2022). *Accountability for NotPetya: Why the International Criminal Court Can, and Should, Prosecute the Perpetrators of the NotPetya Cyber Attack as a War Crime*. The International Criminal Court Forum. https://iccforum.com/forum/cyberwar

Mundi, J. (n.d.-a). *Wiki Note: Due Diligence*. https://jusmundi.com/en/document/publication/en-due-diligence-1

Nagpal, R. (2008). *Introduction to Indian Cyber Law*. Asian School of Cyber Law. http://osou.ac.in/eresources/introduction-to-indian-cyber-law.pdf

Ning, H. (2022, April 6). *A Brief History of Cyberspace*. Routledge & CRC Press. https://www.routledge.com/A-Brief-History-of-Cyberspace/Ning/p/book/9781032078328

Obama, B. (2011). *INTERNATIONAL STRATEGY FOR CYBERSPACE*. THE WHITE HOUSE WASHINGTON. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

On the Application of International Law in Cyberspace. (2011). Auswärtiges Amt. https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

Radpey, L. (2022, April 24). *The Violations of Sovereignty and the Right to Self-Determination in Rojava and Ukraine*. Opinio Juris. https://opiniojuris.org/2022/04/25/the-violations-of-sovereignty-and-the-right-to-self-determination-in-rojava-and-ukraine/

Reich, P. C. (2010). *Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents -and the Dilemma of Anonymity*. Mendeley. https://www.mendeley.com/catalogue/fb25deed-b474-3d47-8911-8475a8184454/

REPORT ON INTERNATIONAL LAW AND CYBERSPACE\. (2021). University of Bologna, University of Milan and University of Westminster. https://www.esteri.it/wp-content/uploads/2021/12/UNIBO_Applicazione-dei-principi-della-Carta-delle-Nazioni-

Unite-nello-spazio-cibernetico.pdf

Rocisini, M. (2019). *GRAVITY IN THE STATUTE OF THE INTERNATIONAL CRIMINAL COURT AND CYBER CONDUCT THAT CONSTITUTES, INSTIGATES OR FACILITATES INTERNATIONAL CRIMES*. Criminal Law Forum (2019) 30:247–272. https://link.springer.com/content/pdf/10.1007/s10609-019-09370-0.pdf

Rodenhäuser, T. (2021). *Cyber Warfare: does International Humanitarian Law apply?* ICRC. https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law

Roland, A. (2009). *War and Technology*. Foreign Policy Research Institute. https://www.fpri.org/article/2009/02/war-and-technology/

Rome Statute of the International Criminal Court. (1998). https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf

Ronzitti, N. (2015). *Respect for Sovereignty, Use of Force and the Principle of Nonintervention in the Internal Affairs of Other States*. European Leadership Network Organisation. https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/ELN-Narratives-Conference-Ronzitti.pdf

Rushing, E. (2022, January 20). *Shifting the narrative: not weapons, but technologies of warfare*. Humanitarian Law & Policy Blog. https://blogs.icrc.org/law-and-policy/2022/01/20/weapons-technologies-warfare/

Schackelford, S. (2010). *STATE RESPONSIBILITY FOR CYBER ATTACKS: COMPETING STANDARDS FOR A GROWING PROBLEM*. Conference on Cyber Conflict Proceedings 2010: CCD COE Publications, 2010, Tallinn, Estonia. https://ccdcoe.org/uploads/2018/10/Shackelford-State-Responsibility-for-Cyber-Attacks-Competing-Standards-for-a-Growing-Problem.pdf

Schjolberg, S. (2012). *Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes An International Criminal Tribunal for Cyberspace (ICTC)*. Cyber Crime Law. https://www.cybercrimelaw.net/documents/ICTC.pdf

Schmitt, M. N. (2017). The use of force (Chapter 14) - Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. In *Cambridge Core*. https://www.cambridge.org/core/books/abs/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/use-of-force/F2871424CF6758F2C9275568B777DF51

Schultz, T. (2008). *Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface*. The European Journal of International Law Vol. 19 no.4. http://www.ejil.org/pdfs/19/4/1662.pdf

Shackelford, S. (2009, April 28). *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1396375

Sigholm, J. (2013). *Non-State Actors in Cyberspace Operations*. Research Gate. https://www.researchgate.net/publication/310827486_Non-State_Actors_in_Cyberspace_Operations#:~:text=Employment%20of%20such%20non%2Dstate,will%20likely%20reshape%20future%20warfare.

Significant Cyber Incidents Since 2006. (n.d.). Center for Strategic and International Studies (CSIS) | Washington, D.C. https://csis-website-prod.s3.amazonaws.com/s3fs-public/220805_Significant_Cyber_Events_0.pdf?ruYyPiNzwADjystZd.g9QgMEPY1K28Et

State responsibility | How does law protect in war? - Online casebook. (n.d.). https://casebook.icrc.org/glossary/state-responsibility

Talem, C. (2020). *INTERNATIONAL LAW IN CYBERSPACE: CYBER ATTACKS AS USE OF FORCE*. CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS). https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2020_Talem_Cecilia.pdf

TANODOMDEJ, P. (2019). *THE TALLINN MANUALS AND THE MAKING OF THE INTERNATIONAL LAW ON CYBER OPERATIONS**. https://10.5817/MUJLT2019-1-4

The Law of Neutrality. (1999). International Law studies-Volume 73. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1558&context=ils

The United Nations Office on Drugs and Crime. (2022). https://www.unov.org/unov/en/unodc.html

The use of force in international law. (2016). The Open University. https://www.open.edu/openlearn/society-politics-law/the-use-force-international-law/altformat-word

Tietsort, J. R. (n.d.). *17 Most Common Types of Cyber Attacks & Examples (2022)*. Aura. https://www.aura.com/learn/types-of-cyber-attacks

Tran, D. (2018). *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*. 20 YALE J. L. & TECH. 376 (2018). https://yjolt.org/sites/default/files/20_yale_j._l._tech._376.pdf

Understanding the International Criminal Court. (n.d.). ICC. https://www.icc-cpi.int/sites/default/files/iccdocs/PIDS/docs/UICCGeneralENG.pdf

United Nations. (n.d.). *United Nations Office on Genocide Prevention and the Responsibility to Protect*. https://www.un.org/en/genocideprevention/crimes-against-humanity.shtml

Use of Force in Cyberspace. (2021). Congressional Research Service (CRS).

https://sgp.fas.org/crs/natsec/IF11995.pdf

Utillano, L. (2020). *International Law and State Cyber Operations*. E Department of International Law of the Secretariat for Legal Affairs of the Organization of American States (OAS). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301834

Vakulyk, O. (2020). *https://www.researchgate.net/publication/340440328_CYBERSECURITY_AS_A_COMPONENT_OF_THE_NATIONAL_SECURITY_OF_THE_STATE*. Journal of Security and Sustainability Issues 9(3):775-784. https://www.researchgate.net/publication/340440328_CYBERSECURITY_AS_A_COMPONENT_OF_THE_NATIONAL_SECURITY_OF_THE_STATE

Vallée, R. (n.d.). *HISTORY OF CYBERNETICS*. SYSTEMS SCIENCE AND CYBERNETICS – Vol. III - History of Cybernetics - R. Vallee. https://www.eolss.net/sample-chapters/c02/E6-46-03-01.pdf

Valuch, J. (2020, December 1). *Use of Force in Cyberspace*. https://sciendo.com/it/article/10.2478/iclr-2020-0023

VON CLAUSEWITZ, C. (1976). *On war*. https://www.usmcu.edu/Portals/218/EWS%20On%20War%20Reading%20Book%201%20Ch%201%20Ch%202.pdf

von Heinegg, W. (2012). *Neutrality in Cyberspace*. 2012 4th International Conference on Cyber Confl Ict. https://ccdcoe.org/uploads/2012/01/1_3_von_Heinegg_NeutralityInCyberspace.pdf

Waxman, M. (2011). *Cyber A Cyber Attacks as &qout;F ttacks as "Force" Under UN Char &qout; Under UN Charter Article 2(4) ticle 2(4)*. Columbia Law School Scholarship Archive.

https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1882&context=faculty_scholarship

Waxman, M. C. (n.d.). *Cyber Attacks as "Force" Under UN Charter Article 2(4)*. Scholarship Archive. https://scholarship.law.columbia.edu/faculty_scholarship/847/

Yong, P. (n.d.). *Comparative research on " Convention on Cybercrime" and Chinese relevant legislation.* https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567%20china-d-Comparative%20Research_ed1a.PDF

Zainab, N., Agung Noviardi, D., & Eka Buana ZK, F. (2018). *Violation on State Sovereignty by Military and Paramilitary Activities on Nicaragua vs United States Case*. SHS Web of Conferences 54, 05001 (2018). https://www.shs-conferences.org/articles/shsconf/pdf/2018/15/shsconf_icolgas2018_05001.pdf

Zainab, N., Noviardi, D., & Buana ZK, F. (2018). *Violation on State Sovereignty by Military and Paramilitary Activities on Nicaragua vs United States Case*. SHS Web of Conferences 54, 05001 (2018). https://www.shs-conferences.org/articles/shsconf/pdf/2018/15/shsconf_icolgas2018_05001.pdf

Newspaper Articles

UHS Hospitals hit by Ryuk ransomware, forced to shut down systems. (2020, September 29). 2020-09-29 | Security Magazine. https://www.securitymagazine.com/articles/93482-uhs-hospitals-hit-by-ryuk-ransomware-forced-to-shut-down-systems

Cyberattack on Continental. (2022). In Continental AG. Retrieved February 13, 2023, from https://www.continental.com/en/press/studies-publications/other-publications/cyber-attack-questions-and-answers/

How the US has helped counter destructive Russian cyberattacks amid Ukraine war. (2022, December 12). In The Hill. https://thehill.com/policy/cybersecurity/3769534-how-the-us-has-helped-counter-destructive-russian-cyberattacks-amid-ukraine-war/

Sayegh, E. (2022, December 13). 2022 In Review: An Eventful Cybersecurity Year. In Forbes. https://www.forbes.com/sites/emilsayegh/2022/12/13/2022-in-review-an-eventful-cybersecurity-year/

International Treaties, Conventions, forums and Papers.

ASEAN CYBERSECURITY COOPERATION STRATEGY (2021 – 2025), https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity Cooperation-Paper-2021-2025_final-23-0122.pdf

Convention on Cybercrime (2001), https://rm.coe.int/1680081561

Convention on the Rights of the Child (1989), https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/crc.pdf

Implementing norms and rules for responsible state behaviour in cyberspace and enhancing cooperation to counter cybercrime. (2022). ICC CYBERSECURITY ISSUE BRIEF #2. https://iccwbo.org/content/uploads/sites/3/2022/03/icc-document-cybersecurity-issue-brief-2.pdf

International Conferences (The Hague), Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land, 18 October 1907, available at: https://www.refworld.org/docid/4374cae64.html [accessed 13 February 2023]

UN. (1998). *Background Materials — Cyberwarfare | International Criminal Court Forum*. The International Criminal Court Forum.

https://iccforum.com/background/cyberwar

United Nations Convention Against Transnational Organized Crime (2000), https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME AND THE PROTOCOLS THERETO. (2004). UN Offie of Drugs and Crimes. https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

الملخص

أصبح التوسع العالمي للإنترنت أسرع وأكثر اتساعًا. وقد أدى ذلك إلى خلق ثورة تكنولوجية قوية ظهرت بشكل أكبر على مر السنين. اليوم ، جمعت الإنترنت كل الجهات الفاعلة في العالم معًا من الدول والأفراد والمنظمات والمجتمعات غير الحكومية والأوساط الأكاديمية والشركات. في الوقت الحاضر ، نرى الدول تعتمد قوتها العسكرية على أنظمة وشبكات الكمبيوتر المتقدمة التي فتحت أمام قوة جديدة. وهكذا ، نرى الآن دولًا تحاول استخدام أنواع مختلفة من القتال الحربي مثل الهجمات الإلكترونية بدلاً من البر أو البحر أو الجو. ومع ذلك ، بالنظر إلى طبيعة وسائل وأساليب الحرب ، فإننا نميل إلى إثارة مسألة شرعية الهجمات الإلكترونية عبر الإنترنت بموجب القانون الدولي.

ومع ذلك ، فإن تطبيق قواعد القانون الدولي على التكنولوجيا والهجمات السيبرانية يمكن أن ينطوي على صعوبة معينة لأن خصائص الهجوم السيبراني تختلف عن نوع الحرب تحت الأرض أو البحر أو الجو. تقدم هذه الأطروحة لمحة عامة عن الموضوعات الأكثر إثارة للجدل في القانون الدولي وتحلل أنواع الهجمات السيبرانية وشرعيتها بموجب القانون الدولي (IL) والقانون الإنساني الدولي والتي تم تقسيمها إلى ثلاثة فصول رئيسية ، مقدمة تقدم لمحة عامة عن المشكلة الرئيسية ، الفصل الثاني الذي يوفر إطارًا قانونيًا وفصلًا ثالثًا يركز على موضوعات القانون الدولي المتعلقة بالهجمات السيبرانية. كان هدفنا الرئيسي هو توفير فهم عام للهجمات السيبرانية ونوعها بالإضافة إلى تطبيق القانون الدولي فيما يتعلق بهذه المسألة. أظهرت النتائج التي توصلنا إليها أن الهجمات الإلكترونية غير قانونية بموجب القانون الدولي وأنها تنتهك السيادة وعدم التدخل وكذلك كل موضوع تقريبًا في القانون الدولي مثل مبدأ التناسب وغيره أيضًا. من منظور السلامة ، تؤكد هذه

الدراسة على الحاجة إلى مراعاة تأثير هذه الهجمات الإلكترونية على سلامة الدولة.

الكلمات الدالة–

الهجمات الإلكترونية ، الحرب الإلكترونية ، الأمن السيبراني ، التجسس السيبراني ، العمليات السيبرانية ، القانون الدولي ، القانون الإنساني الدولي ، الدول ، الجهات الفاعلة غير الحكومية ، المنظمات ، السيادة ، عدم التدخل.