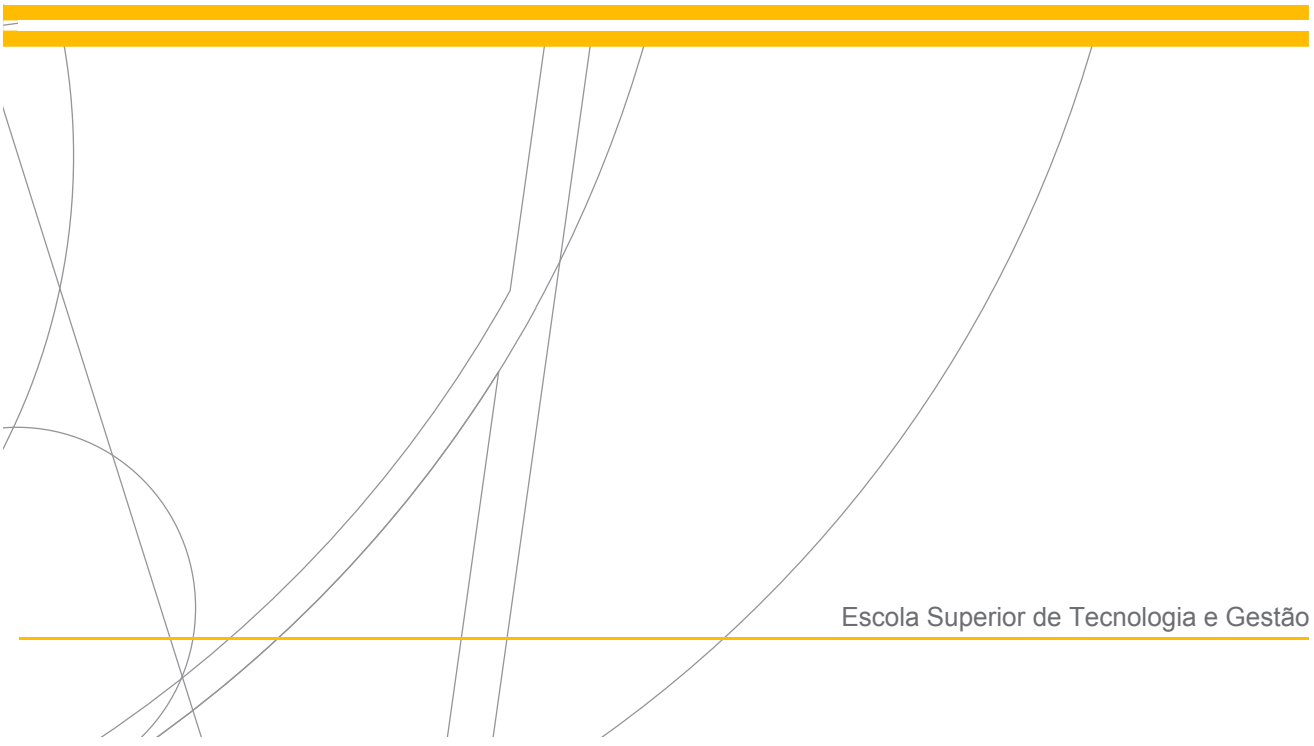
Instituto Politécnico
de Viana do Castelo

CIBERGUERRA

Uma Nova Era da Guerra

Sara Pinheiro



Escola Superior de Tecnologia e Gestão

Instituto Politécnico
de Viana do Castelo

Autor(a)

SARA LINDA DE ALMEIDA PINHEIRO

Trabalho efetuado sob a supervisão de

Professor Luís Manuel Cerqueira Barreto

Professor Rogério Matos Bravo

Mestrado em Cibersegurança

Julho de 2024

Mestrado em Cibersegurança
Master in Cybersecurity

Cyberwarfare: A New Era of Waging War

a master's thesis authored by

Sara Linda de Almeida Pinheiro

and supervised by

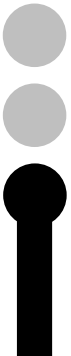
Luís Manuel Cerqueira Barreto
Professor Coordenador, IPVC

Rogério Matos Bravo
Professor Adjunto Convidado, IPVC

This thesis was submitted in partial fulfilment of the requirements for the Master's degree in Cybersecurity at the Instituto Politécnico de Viana do Castelo

ipvc

30 of September, 2024



Abstract

As the technological world continues to evolve, so does the type of infrastructures management a nation has, since they are more connected via computer systems. In doing so, if one wants to wage war against a nation, instead of starting by destroying its essential structures by deploying several resources, this can be done by a "simple" cyberattack of its infrastructures' systems – which can be done remotely. These types of attacks can cause significant damage to a nation's vital systems and be compared directly with the ones sustained by an actual kinetic attack. This dissertation will focus on the evolution of Cyberwarfare and its impact on society. Considering those are very modern and recent concerns, it is important to understand which laws and regulations on cyberwarfare and cybercrime exist in the international context. Even though there are multiple laws and regulations related to cyberspace, until now there is no specific legislation dedicated to Cyberwarfare.

Keywords: Cyberwarfare. Cyber Law. Cyberattack. Cybercrime.

Resumo

À medida que a tecnologia continua a evoluir, a gestão das infraestruturas de uma nação também se desenvolve, uma vez que estão cada vez mais interligadas através de sistemas informáticos. Assim, em vez de destruir as estruturas essenciais de uma nação com recursos físicos, é possível realizar um "simples"ciberataque aos sistemas das suas infraestruturas - de forma remota. Estes ataques podem causar danos significativos aos sistemas vitais de uma nação, podendo ser comparados aos provocados por um ataque físico direto. Neste trabalho, será abordada a evolução da Ciberguerra e o seu impacto na sociedade. Dado que são preocupações bastante atuais e recentes, é fundamental compreender as leis e regulamentos referentes à ciberguerra e cibercrime num contexto internacional. Ainda que existam múltiplas leis e regulamentações relacionadas ao ciberespaço, até agora não há uma legislação específica dedicada à Ciberguerra.

Palavras-chave: Ciberguerra. Ciber Leis. Ciberataque. Cibercrime.

Aknowledgements

I express my sincere appreciation to Professor Luís Barreto and Professor Rogério Bravo for entrusting me with the opportunity to commence this thesis journey and for guiding me through the world of research and academia with expertise.

I am grateful to Professor Pedro Pinto for enabling me to join the Cybersecurity Master's program and for supporting me in bridging my knowledge from Forensic and Criminal Sciences to the Cyber domain in my thesis. Your mentorship has been invaluable in shaping my academic pursuits, and I thank you for providing me with these enriching opportunities.

I wholeheartedly dedicate this thesis to my Mother, whose unwavering support, patience, and care have been the bedrock of my academic pursuits and in my life. To my Nonna, whose wisdom and love have provided me with invaluable guidance and strength throughout this journey. And to my sisters, Mariana and Catarina, whose laughter and companionship have brought joy and resilience to every step of this endeavor.

Contents

List of Figures

List of Abbreviations

North Atlantic Treaty Organization (NATO) CCD COE NATO Cooperative Cyber Defence Center of Excellence

C&C Command-and-Control

CFAA Computer Fraud and Abuse Act

CoE Council of Europe

DDoS Distributed Denial of Service

DoS Denial of Service

ESTG Escola Superior de Tecnologia e Gestão

ICRC International Committee of the Red Cross

ICSs Industrial Control Systems

ICT Information and Communication Technology

IHL International Humanitarian Law

IIL Institute of International Law

IPVC Instituto Politécnico de Viana do Castelo

LOAC Law of Armed Conflict

NATO North Atlantic Treaty Organization

People's Liberation Army PLA

PLCs Programmable Logic Controllers

T-CY Cybercrime Convention Committee

UK United Kingdom of Great Britain and Northern Ireland

UN United Nations

USA United States of America

Chapter 1

Introduction

"Peace cannot be kept by force; it can only be achieved by understanding."

Albert Einstein

The 21st Century marked a new era for making war. Battlefields are no longer constricted to geographical and physical barriers due to the technological advances made in the information and communication technologies. Nowadays, the use of the Cyber Space to carry out attacks is way more inexpensive than kinetic attacks (physical attacks), as all the tools needed to do so are available online. Furthermore, these attacks can be launched from anywhere to everywhere around the globe and may cause massive loss, may it be infrastructures - communication, health systems, or others -, financial, or human lives[2].

Cyber Space has been recognised by many has the fifth domain of war - the other four being land, sea, air, and space[4]. The North Atlantic Treaty Organization (NATO) also recognizes cyberspace as an "official domain of warfare"[22]. However, this new domain presents many challenges mainly about what are the limits and boundaries of this battlefield. Moreover, this battlefield presents all actors involved - private individuals, organized crime, extremist groups, and state actors - alike access to resources and means to carry out attacks. These actors can affect the defenses and economies of sovereign states and even target private individuals and firms[61].

To better understand what Cyberwarfare is, it is important to understand what war is, as classifying a conflict as War is vital to determine which laws and rules are relevant[47].

1.1 Motivation

In a world mainly managed through cyberspace, this domain is bound to become the main player in war and, most likely, even becoming the most sought after battlefield as it leads to a type of war that can be waged with very little money in comparison to "normal" war. This easiness in making war is very worrying as it hides and detaches the human component of it all, making this a very emergent topic to be researched and discussed.

1.2 Objectives

This thesis aims to explore two key questions: *How has the concept of war evolved?* And, *are there any specific laws or regulations that pertain to cyberwarfare?* Thus, the two key questions are addressed through exploratory research, which involves gathering accessible information by tracking clues, using available links, exploring law-related websites, and referencing publications.

1.3 Cyberwarfare

In the book The Art of War, Sun Tzu describes war as of being "of vital importance to the Sate. It is a matter of life and death, a road either to safety or to ruin. Hence it is a subject of inquiry which can on no account be neglected". It is important to notice that sayings in this book have been spoken by General Sun Tzu in the 5th century BC[35]. Over the centuries many authors defined war differently, however all agree that war is an act of violence that involves the killing and disabling of humans[47]. Francisco Suárez (1548-1617) defined war as being a "contest at arms which is incompatible with external peace" and is "carried on between two sovereign princes or between two states"[62]. Alberico Gentili (1552-1608) completed Suárez definition by adding that "war is a just and *public* contest of arms", and that "much is accomplished in war without the use of arms, yet there is never a war without the *preparation* of arms". Gentili also stated that war "must be public; for war is not a broil, a fight, the hostility of individuals". This contest of arms, described by Suárez and Gentili, and many others, it is referred to the use of arms by all parties involved directed at the lives of opposing soldiers and not at property[47].

Hugo Grotius (1583-1654) also includes the concept of arms for defense and offense purposes, and that arms are "used by just man for defense and [lawful] acquisition, by the unjust man, for attack and seizure". The conflicts involving arms by all parties is designated War[37]. Later on, Grotius expands his definition by also taking into account "contests of force" and not just the ones that use arms. Grotius also adds that war is not a "contest but a condition", which might imply that he thought of war as a state of affairs that goes on for a time, comprising more than a "single act of contesting" distancing the definition of war from the definitions of duel, jousting matches and other contests of force that happen with just one event and between single parties[47][36].

The present-day author Brian Orend (1971) defines war as "an actual, intentional and widespread armed conflict between political communities"[48].

All definitions found about war make it as something violent, organized, and done "to bring the fulfillment" of the *war wager*'s will, it is not done with the sole purpose of killing[4]. War is also a **public event** between parties.

Oxford English Dictionary defines Cyberwarfare as "the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes". This definition simply defines the concept of cyberwar, but does not comprehend the scope and problematic of what is cyberwar and how to classify a cyber "event" as cyberwar or merely a cyberattack. For that it is needed to take the previous stated definitions of war and broaden its meaning to include the cyber complexity of it.

In Gentili's definition of war, he states that war is a *constest of arms* or weapons. This definition can be extrapolated to cyberwar as the use of cyberattacks can be described as some type of contest using a sort of weapon. This weapon being a destructive computer program placed in secret in a foreign computer system[47]. However, this placement is done clandestinely taking off the public question out of this event. If the cyberattack is done publicly it will lose its effect, as in part, for a fully successful cyberattack to occur it needs be in secret, otherwise, the target of the attack will, most likely, be able to prevent it. This raises the question if Cyberwar is actually the act of War or if it is just a cyberattack, since one of the main principles of War is being a public contest.

On the other hand, it is important to consider Suárez's definition which states that

war is an attack between two sovereign states and the attack crosses state lines. Well, a cyberattack that crosses sovereign state lines with the intent of causing disruption to that state's infrastructures and military systems may be consider an act of war.

Other authors have been writing and thinking about what is cyberwar, completing this definition and defining what is this new battlefield - **Cyberspace** - which encompasses a complex domain formed by the interconnected networks of information technology infrastructure and stored data, encompassing components such as the internet, telecommunications networks, computer systems, and embedded processors and controllers[61][53]. Straub and Traylor attested to the nonexistence of a physical space and boundaries in which this type of war is fought, and the fact that there are "no physical assets to attack or defend and no potential for a kinetic attack to traverse this medium to attack others"[61].

Cyberspace knows no conventional boundaries or borders, enabling clandestine cyberattacks to strike from vast distances, it is crucial to recognize that the impact of cyberwarfare can be as lethal, if not more so, than traditional forms of warfare.

Susan W. Brenner defines cyberwar as "actions taken by states using technology with a view to achieve military or other strategic goals", differentiating from cyberterrorism, which D. Dennings defines as "unlawful attacks and threats of attacks against computers, networks, and information collected in networks to intimidate or coerce governments, or the residents, of a given state, to fulfil political or social objectives". For an attack to be considered as cyberterrorism, its result should be violence against people and property, or even induce fear caused by the magnitude of harm[55]. The main difference between cyberwar and cyberterrorism lies in their *objectives* and *actors involved*[68].

There have been some concerns about when a cyberattack can be considered an act of war, and what are the possible/appropriate responses available for victim nations. Cyberattacks may be carried out by various actors, while cyberwar is mainly associated with nation-state actors engaging in warfare in cyberspace. Their main difference are their *scope* and *scale*[68].

Another concept that is fairly important for all these distinctions is *cybercrime*, in which the perpetrator breaches networks unauthorized and steals intellectual property and other data. These crimes can be financially motivated, and response lies usually in

the jurisdiction of law enforcement agencies[68].

Chapter 2

History of Cyberwar

China is identified as one of the initial nations to advance the development of cyberwarfare capabilities. In 1975, Ye Jianying (a founding member of the PLA (People's Liberation Army)) delivered a report titled "Strengthening Electronic Countermeasure Work" to the Central Committee of the Communist Party of China. Ye's report documented how China could use electronic warfare as a weapon to strengthen its military force and increase its position as a major world power. Heeding his recommendations, the Chinese government established the People's Liberation Army Electronic Engineering College in 1979, dedicated to instructing soldiers on how to jam, deflect, and bypass electronic radar communications. Subsequently, years later, the National Defense Science and Technology University's School of Electronic Countermeasure initiated its program to educate and prepare PLA soldiers in electronic warfare tactics. This training program equipped soldiers with an understanding of computer and network usage, with a special focus on areas such as offensive computer operations that are still crucial to today's cyber operations. It is important to note that since then China has executed a cyber-espionage program considered to be one of the most successful on the global stage[22].

John Arquilla and David Ronfeldt are amongst the first to introduce the cyberwar concept to the world in the 1990s. They were concerned how technology evolution was going to affect warfare scenarios as cyberwar would most likely have "implications for integrating the political and psychological with the military aspects of warfare", and so it should not be taken lightly and confused with computerized, automated, robotic, or electronic warfare[5]. Not long after their warnings a significant cyberconflict began.

The *Kosovo War* (February 1998 - June 1999) has been described as the first war on the Internet. Both government and non-government actors used the cyberspace to "disseminate informaion, spread propaganda, demonize opponents, and solicit support for their position". Several pro-Serbia hacker groups - including the *Black Hand* - attacked NATO's Internet infrastructure, disrupted services on government computers and took over their Web sites. These attacks mainly happened via Denial of Service (DoS) and e-mail infected with viruses[20][33].

In 1999 began *The Palestinian-Israeli Hacker Conflict* which by the end of September 2000 had escalated to a full on Cyberconflict[3]. After three Israeli soldiers were abducted in October of 2000, the *Hizballah* website got hacked and Israeli flags and sound file with the Israeli anthem were planted on the website. Following this, pro-Israel hackers attacked "official websites of military and political organisations perceived as hostiles to Israel, including the Palestinian National Authority, Hamas, and Iran". In return, pro-Palestine hackers retaliated by hitting Israeli political, military, telecommunications and universities websites and infrastructures[33]. From October 2000 to the end of January 2001 more than 160 Israeli and 35 Palestinian websites had been struck. The main attacks used were website defacement - mainly targeting prominent political websites, including those of governmental entities - and Distributed Denial of Service (DDoS) - disabling rival websites for days, further burdening the Internet infrastructure in the area[3]. Since 2000, this cyberconflict has often paralleled the kinetic conflicts. In 2006, during heightened tensions between Israel and Gaza, pro-Palestinian hackers disrupted roughly 700 Israeli Internet domains, including those belonging to Bank Hapoalim, Bank Otsar Ha-Hayal, BMW Israel, Subaru Israel, and McDonald's Israel[33].

The Estonian government decided to relocate a Soviet Red Army war memorial statue in Tallinn erected for the "Soviet troops who died while taking it in World War II". This monument had been the center of tensions between pro-Kremlin and Estonians nationalist movements, as for the first it represented "liberator" and for the second "oppressor"[49]. The works for the removal of the statue started on April 26 2007 with many protests accompanying it. The next day, Estonia fell under several cyberattacks that lasted 22 days (April 27 - May 18) impeding the country to function normally. On April 27, numerous important Estonian websites experienced a significant DDoS attack. These attacks

were directed at web, DNS[1], SQL[2], and email servers across Estonia disrupting the infrastructure of government, telecommunications, law enforcement, media organizations, and financial institutions, resulting in the unavailability of critical services to the public[22]. Despite the lack of claims or admission from the Russians regarding these attacks, multiple indicators hinted otherwise. The malicious traffic frequently showed clear signs of political motivation and originated from a Russian language background. Additionally, detailed instructions for targeting Estonian sites, including motivation, targeting, and timing information, were circulated in various Russian language forums and websites[49].

Following a long standing conflict between Russia and Georgia over territory, in mid-July 2008 with the growing tensions between the two countries it became evident an escalation of the events to the cyberspace. Starting on August 8, multiple Command-and-Control (C&C) servers[3] targeted Georgian websites, including those of the Georgian President, central government, Ministry of Foreign Affairs, and Ministry of Defence, as well as non-Georgian platforms sympathetic to Georgia, like news sites and online forums. On August 9, Georgia's largest commercial bank (TBC) was targeted. On August 10, the Georgian Parliament and President's website were stroked by http-flood attacks. The Georgian Ministry of Foreign Affairs released a statement on August 11, reporting that a cyberwarfare campaign led by Russia was causing severe disruptions to numerous Georgian websites, including the Ministry of Foreign Affairs site. For 3 weeks (August 8 - August 28) Georgia was under intense cyberattack, in which the attackers resorted to:

- "DoS and DDoS attacks;
- Distribution of malicious software (MS batch script) together with attack instructions - exploiting SQL vulnerability;
- Defacement;
- Using e-mail addresses for spamming and targeted attacks."

[1]Domain Name System (DNS) is the phonebook of the Internet[72]

[2]Structured Query Language (SQL) is a standardized language used to interact with relational databases[41]

[3]A command-and-control server (C&C server) is a computer that sends commands to compromised digital devices, like those infected with rootkits or ransomware.[8]

All of the attacks were meant to target government websites, news and media websites and financial institutions.[69]

The cyber conflicts discussed, have been confined to cyberspace, but their impacts extend into the real world, disrupting a country's functioning by targeting critical infrastructures like banks (financial/economic sector), media outlets (information dissemination), and government institutions, affecting organization and operations. These infrastructures form the foundation of a nation's functionality; their disruption can lead to chaos and disorder, essentially equating an attack on them to a direct assault on people's freedom, potentially seen as an act of war.

In May 2010, a *Cyber Weapon* named *Stuxnet* disrupted Iran's nuclear program by targeting centrifuges at the Natanz Fuel Enrichment Plant. The malware, likely developed by a nation-state attacker, used advanced exploits to infiltrate the plant's systems. Due to tensions over Iran's nuclear goals, the United States of America (USA) came under suspicion for this attack. *Stuxnet* spread via USB devices strategically placed at affiliated organizations linked to the plant targeting its centrifuges, sabotaging the systems responsible for uranium enrichment by causing them to spin out of control and damaging crucial equipment[22].

Stuxnet is a truly remarkable piece of malware with historical significance for several reasons:

1. *Stuxnet* is recognized as the inaugural malware to inflict tangible, real-world damage, effectively blurring the lines between the cyber and physical domains and signaling the advent of a new chapter in the domain of cyberwarfare.

2. It exploited multiple zero-day vulnerabilities (four affecting the operating system and one affecting an application) and used valid digital certificates to appear as if issued by trusted parties, which was unprecedented in malware history.

3. The precision targeting of *Stuxnet*, which combined elements of cyber intelligence with cyber sabotage, rendered the origins of the attack virtually untraceable, obscuring the identities of its creators.

4. *Stuxnet* was engineered to compromise specific Siemens Programmable Logic Con-

trollers (PLCs) that are employed in Industrial Control Systems (ICSs), particularly those associated with the uranium enrichment process.

5. The malware was capable of both reporting to and receiving updates from a C&C server, showcasing its advanced capabilities in data exfiltration and self-upgrading.

6. *Stuxnet* was designed with built-in fail-safes, including a self-termination date and constraints on its propagation, to manage its dissemination.

7. Despite its advanced design, *Stuxnet* was not without flaws, as evidenced by bugs in its code, indicating that even sophisticated malware can suffer from programming oversights[17].

In essence, *Stuxnet* represents a critical turning point in the history of cyber threats, illustrating that malware can have direct and destructive effect on vital infrastructure, carrying profound repercussions for national security and shaping the future course of cyberwarfare.

Furthermore, Stuxnet inspired the creation and improvement of cyberweapons. An example of this is *Duqu*, a complex cyber threat recognized as a precursor to the Stuxnet worm, with its main focus being espionage rather than sabotage. It was initially reported on October 14, 2011, by the CrySyS Laboratory at Budapest University of Technology and Economics. Duqu's primary objective is to gather intelligence from various organizations, particularly those involved in industrial infrastructure and system manufacturing. This information aids in planning future attacks by offering insights such as design documents. It is believed that Duqu was developed by the same authors as Stuxnet or by individuals with access to its source code[7]. CrySys Laboratory also found sKyWIper, a highly advanced cyber-espionage malware created for extensive data gathering from specific systems, frequently linked to nation-state operation mainly deployed in the Middle East since 2010[63][45].

Chapter 3

Laws and Regulations

The first attempt at stipulating laws of war was made in 1863 by Professor Francis Lieber during the American Civil War and disseminated and enforced by the President of USA, Abraham Lincoln. Even though the *Lieber Code* was only valid for USA, these set of instructions/rules marked the starting point of the creation of *Laws of War*, as they influenced other states to adopt and create similar regulations. Furthermore, the Lieber Code jump started the project of an international convention on the laws of war later presented in the Brussels Conference in 1874 - *Project of an International Declaration concerning the Laws and Customs of War. Brussels, 27 August 1874* [40][54].

Prior to the Brussels Conference, in October 1863 happened the Geneva International Conference where was founded the *International Relief Committee for Injured Combatants*, which adopted, in 1875, the name *International Committee of the Red Cross (ICRC)*. This conference was held with the purpose of insisting that governments should support relief committees, medical corps, ambulance services and military hospitals during war, protecting medical staff and the injured[57]. In 1864, the Geneva Committee assembled again, inviting the governments of all European and several American states, to lay down some principles relating to the treatment of the wounded in the field of battle:

- relief to the wounded without any distinction as to nationality;
- neutrality (inviolability) of medical personnel and medical establishments and units;
- the distinctive sign of the red cross on a white ground.

In 1868, these principles were revised to adapt them to sea warfare as well[14][1].

In 1873 was founded the Institute of International Law (IIL), with the objective of assisting in the advancement of international law by striving to articulate the fundamental principles of the field and by providing aid in the gradual and progressive codification of international law[64].

The first attempt to an international agreement on the laws and customs of war was made in 1874, Brussels. However, since there was no accordance between the governments to accept it as rule, it was not approved[54].

On September 9 1880, the IIL gathered for a session in Oxford, and created the *The Laws of War on Land*, with the purpose of establishing guidelines and principles on how to behave when conducting warfare, by emphasizing the importance of respecting the rights and dignity of all individuals involved in warfare[27].

From this point, there were several gatherings, conferences and conventions with the objective of further discussing what is acceptable in the act of war and what is not. There were several rectifications to better the previous approved regulations and laws in order to include the evolution of the means of war and its technology, such as naval warfare and the use of balloons to deploy projectiles and explosives.[11][12][18].

The Hague Conventions from 1899 and 1907 originated the informal term of the *Law of the Hague*, that regulated the implementation of warfare strategies, management of hostilities, and processes of occupation[42].

In February of 1909, the Ten Sea Powers (Austria-Hungary, France, Germany, Italy, Japan, Netherlands, Russia Federation, Spain, the United Kingdom of Great Britain and Northern Ireland (UK), and the USA) convened in London to make decisions regarding the International Prize Law[19].

The IIL adopted on August 9 1913 the *Manual of the Laws of Naval War*, which stated that its laws were only relevant in high seas and within the territorial waters of the parties involved in the conflict[26].

After World War I ended, a conference was held in Washington, USA (February 1922), about the *Limitation of Armaments*, where the USA, the UK, France, Italy, and Japan discussed a treaty regarding the *Use of Submarines and Noxious Gases in Warfare*. However it did not entered into force, as there were some concerns about the provisions on submarine warfare[71]. In this conference was also formed a Commission of Jurists tasked

with the development of regulations pertaining aerial warfare and the use of radio in time of war. This commission met at the Hague from December 1922 to February 1923. They released a two-part report - Part I concerning the control of radio in time of war and Part II about the rules of air warfare - in which the rules were never adopted in legally binding form as they correspond significantly with the traditional norms and fundamental tenets that form the basis of the established treaties on land and maritime warfare[58].

The *Diplomatic Conference of 1929* was convened in Geneva, Switzerland, with the purpose of revising the Geneva Convention of 1906, specially concerning the *Wounded and the Sick in Armies in the Field* as well as updating the terms contained in the Hague Regulations of 1899 and 1907 regarding the *Treatment of the Prisoners of War*, which the First World War (1914-1918) uncovered various flaws and a discernible need for increased specificity[31][15][13].

In 1934 there were two draft conventions one in Monaco and one in Tokyo, Japan with the intention of the conclusions being presented in the Diplomatic Conference that was to happen in the beginning of 1940 but due to the outbreak of the Second World War (1939-1945) were only presented at the Diplomatic Conference of 1949 and inserted in the *Geneva Conventions of 1949*[32][24].

From 1941 to 1945 there were several meetings and conferences between various state nations world wide to figure what they could do regarding the Second World War and what would be the post-war future. These meetings were all in preparation of the San Francisco Conference, also known as the *United Nations Conference on International Organization* (April 25 - June 26 1945), where representatives of 50 nations attended to constitute the *United Nations (UN)*. For the following two months they proceeded to draft the Charter of the UN and then sign it. This Charter entered in force on October 24 1945[39][43][66].

The Diplomatic Conference of Geneva that was suppose to happen in 1940, was finally held nine years later, in 1949. The Conference convened for the purpose of revising:

- the Geneva Convention of 27 July 1929 for the Relief of the Wounded and Sick in Armies in the Field,
- the Xth Hague Convention of 18 October 1907 for the Adaptation to Maritime Warfare of the Principles of the Geneva Convention of 6 July 1906,

- the Geneva Convention of 27 July 1929 relative to the Treatment of Prisoners of War,

and to establish a Convention for the Protection of Civilian Persons in Time of War (21 April - 12 August 1949), at Geneva, based on the four Draft Conventions scrutinized and endorsed by the XVIIth International Red Cross Conference held at Stockholm[30].

The Conference set forth the texts for the following Conventions:

I. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field.

II. Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea.

III. Geneva Convention relative to the Treatment of Prisoners of War.

IV. Geneva Convention relative to the Protection of Civilian Persons in Time of War.

Since the implementation of these conventions, there have been a few additional protocols and amendments, between 1977 and 2005[34].

In 2001, the Council of Europe (CoE) convened in Budapest with member and non-member States to establish the *Convention on Cybercrime* (ETS No. 185), commonly referred to as the *Budapest Convention*. This treaty focuses on combatting cybercrime challenges via international collaboration, setting a standard for member States to align national laws, enhance investigative methods, and foster cross-border cooperation in addressing cybercrime[16].

The cyberattacks against Estonia (2007) and Georgia's (2008) government, media, banking, and political party websites led to the invitation of an 'International Group of Experts' (2009) by NATO Cooperative Cyber Defence Center of Excellence (NATO) to examine "how extant legal norms applied to this 'new' form of warfare" resulting in the *Manual on the International Law Applicable to CyberWarfare* most commonly know as *Tallinn Manual*. It is important to note that this document is a non-binding set of guidelines on how to apply existing laws to the 'cyber world'. The Tallinn Manual was originally published in 2013[60].

3.1 The Beginning of Cyberlaws

The evolution of computational resources and digital globalization has fostered a surge in cybercrime, underscoring the imperative for legal frameworks to counter illicit behaviours in the virtual domain. Canada stands out as one of the pioneers in enacting early legislation to tackle cyber offenses.

In the late 1970s in Canada, computers began to be utilized for illicit activities. However, existing laws inadequately addressed these emerging forms of criminality. Offenders were commonly prosecuted for fraud or theft, as legal frameworks did not encompass computer-related crimes[38]. This legislative gap necessitated the amendment of the Criminal Code in 1983 to introduce section 342.1 - *Unauthorized use of computer*, which states:

> **342.1 (1)** Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction who, fraudulently and without colour of right,
>
> **(a)** obtains, directly or indirectly, any computer service;
>
> **(b)** by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;
>
> **(c)** uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system; or
>
> **(d)** uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c). [...][44]

In 1984, the USA introduced the *Computer Fraud and Abuse Act (CFAA)* amending the Federal Criminal Code to establish offenses related to unauthorized computer usage. This law prohibits the unauthorized access or misuse of computers with the intent to defraud, encompassing actions that alter, destroy, disclose information, or impede the rightful use of government-operated

computers[70]. Two years later the CFAA was revised to address hacking activities[10] and to adjust the scope of conduct that the law covers, and revisions to the penalties for violations[23].

The UK enacted the *Computer Misuse Act* in 1990, encompassing laws that criminalize unauthorized access to computer material, actions intended to disrupt computer functioning, and other related offenses. It also establishes jurisdictional parameters and penalties for such violations[50].

In 1993, Singapore passed the *Computer Misuse Act (Chapter 50)* to safeguard computer material against unauthorized access or alterations, with provisions addressing a range of offenses, including:

- Unauthorized access to computer material (Section 3).
- Access with intent to commit or facilitate the commission of an offense (Section 4).
- Unauthorized modification of computer material (Section 5).
- Unauthorized use or interception of computer service (Section 6).
- Unauthorized obstruction of the use of a computer (Section 7)[56].

China established its initial cybercrime legislation framework through the *Ordinance on Protecting the Safety of Computer Systems* (1994), which aimed to safeguard computer systems from unauthorized access and other security breaches. Subsequently, in 1997, China amended its Penal Code to include Articles 285, 286, and 287, targeting specific cybercrimes like illegal system access, system sabotage, and the facilitation of such crimes. These amendments were part of China's proactive measures to tackle the rising threat of cybercrime[52].

In 1996, Russia included the "Crimes in the Sphere of Computer Information" section in the Criminal Code of the Russian Federation, creating a distinct chapter focused on offenses related to computer systems and information technology. Introduced alongside the new Criminal Code in 1996, this chapter

has undergone several amendments over the years to align with the changing landscape of cybercrime. This chapter initially included provisions such as:

- Article 272: Illegal Accessing of Computer Information
- Article 273: Creation, Use, and Dissemination of Harmful Programs for Electronic Computer Machine
- Article 274: Violation of Rules for the Operation of Electronic Computer Machine

These articles criminalized unauthorized access to computer information, the creation and distribution of malware, and the violation of operational rules for computer systems[25].

In 1987, Japan made revisions to its Penal Code to combat the rise of computer-related crimes, safeguard electronic fund transfers, and protect computer programs and electronic data integrity. The amendments introduced specific cyber offenses including:

- Illegal production of electromagnetic records,
- Interference with business transactions through computer systems,
- Computer fraud,
- Destruction of electromagnetic records.

These changes aimed to criminalize actions that disrupt or misuse computer systems, especially within a modern business setting. However, Japan's first dedicated cybercrime law was the *Unauthorized Computer Access Law (Law No. 128 of 1999)*, which targeted unauthorized access to computer systems, particularly those accessed through telecommunication lines[46].

Australia's Cybercrime Act 2001 establishes a comprehensive legal structure to combat cybercrime. It defines and criminalizes unauthorized data access, imposes penalties for severe computer offenses, empowers law enforcement with specific data access abilities, exempts intelligence agency personnel from li-

ability for actions outside Australia, and updates legal references to address unauthorized system access. Some of the offenses included in this Act are:

- Unauthorized access, modification, or impairment with intent to commit a serious offense (Section 477.1)
- Unauthorized modification of data to cause impairment (Section 477.2)
- Unauthorized impairment of electronic communication (Section 477.3)
- Unauthorized access to, or modification of, restricted data (Section 478.1)
- Possession or control of data with intent to commit a computer offense (Section 478.3)
- Producing, supplying, or obtaining data with intent to commit a computer offense (Section 478.4)[21]

These statutes represent some of the earliest enactments, with numerous subsequent laws emerging to align with technological progress and the concurrent surge in cybercrime. The identification of legislative deficiencies, whether at an individual or collective level, accentuates the imperative for nations to partake in communication, collaborative efforts, and implement measures to fortify their protective and responsive capacities.

3.2 The Budapest Convention

The *Budapest Convention*, formally referred to as the *Convention on Cybercrime*, stands as an international treaty formulated by the CoE to confront the challenges arising from the increasing prevalence of cybercrime. The Convention serves several key purposes:

1. **Harmonization of Domestic Criminal Law**: It seeks to coordinate and standardize the national criminal statutes of signatory nations concerning crimes involving computer systems and data, promoting a cohesive approach to combating cybercrime globally.

2. **International Cooperation**: The Convention sets the groundwork for international collaboration among participating entities to enhance the investigation and prosecution of cybercrimes effectively. This encompasses extradition agreements, mutual aid, and the sharing of evidence in electronic form.
3. **Protection of Human Rights**: The Convention acknowledges the necessity of harmonizing law enforcement objectives with the safeguarding of fundamental human rights, including freedom of expression, privacy, and the protection of personal data, as outlined in various international agreements.
4. **Procedural Law and Law Enforcement**: It provides for the adoption of procedural laws that enable the collection, preservation, and use of electronic evidence in cybercrime investigations and proceedings.
5. **Supplementation to Existing Treaties**: The Convention enhances efforts to combat cybercrime by complementing current international treaties on criminal cooperation, like the European Convention on Extradition and the European Convention on Mutual Assistance in Criminal Matters.

As the first treaty dedicated to addressing Internet and computer crimes through the alignment of national laws, enhancement of investigative methods, and promotion of international cooperation, this Convention was signed in Budapest on November 23, 2001, marking a pivotal milestone in the worldwide effort to combat cybercrime[16].

The Budapest Convention is succeeded by two additional protocols:

- Additional Protocol to the Convention on Cybercrime (ETS No. 189), concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (2003)
- Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (2021)

The main objective of the Additional Protocol to the Convention on Cybercrime is to complement the Convention by specifically addressing the criminalisation of acts of a racist and xenophobic nature perpetrated through computer systems. This involves defining offenses concerning the spread of racist and xenophobic content, threats, insults, as well as the denial or downplaying of genocide or crimes against humanity when done deliberately through computer systems. The Protocol strives to standardize legal reactions to these actions while upholding a equilibrium with the principles of freedom of expression[28].

The Second Additional Protocol to the Convention on Cybercrime complements the original Convention and the First Protocol by offering additional tools to enhance cooperation and facilitate the disclosure of electronic evidence in specific criminal investigations or legal proceedings. These entail provisions for more effective mutual assistance and diverse forms of collaboration among competent authorities, emergency cooperation during situations posing significant and immediate risks to life or safety, and direct engagement between authorities and relevant service providers possessing pertinent information. The Protocol strives to bolster law enforcement capabilities in combating cybercrime and other offenses involving electronic evidence while upholding human rights and fundamental freedoms. It also emphasizes the importance of an internet that allows the free flow of information and incorporates safeguards for protecting personal data transferred under the Protocol[29].

The Cybercrime Convention Committee (T-CY) was formed alongside the Convention on Cybercrime playing a vital role in ensuring the Budapest Convention remains dynamic, adapting to the changing realm of cybercrime. Functions and contributions of the T-CY include:

1. **Assessment of Implementation**: The T-CY is responsible for assessing the implementation of the Convention by its Parties,which includes reviewing how effectively member states have integrated the Convention's provisions into their domestic laws and the practical enforcement of these regulations.

2. **Guidance and Interpretation**: The T-CY develops Guidance Notes to aid Parties in in understanding and applying the Convention. These notes serve as authoritative references to clarify the treaty's provisions, ensuring uniform and efficient implementation across diverse jurisdictions.
3. **Capacity Building**: The T-CY, supported by the specialized Cybercrime Programme Office (C-PROC), nables international capacity-building initiatives. These projects are designed to assist countries in establishing crucial legal frameworks and enhancing their law enforcement capabilities to combat cybercrime effectively on a global scale.
4. **Evolution of the Convention**: Through the T-CY, member states actively contribute to the ongoing development of the Budapest Convention. This includes the development of additional protocols, like Second Additional Protocol.
5. **Networking and Cooperation**: The T-CY gain access to practitioner networks like the 24/7 contact point network, fostering trusted cooperation and information exchange among countries. This collaboration proves especially beneficial during emergencies and in addressing specific instances of cybercrime.
6. **Legal Basis for Cooperation**: The T-CY secures the Convention as a legal framework for international cooperation in cybercrime and electronic evidence. This involves aiding mutual legal assistance, extradition, and spontaneous information exchange among Parties.
7. **Private Sector Engagement**: The efforts of T-CY has enhanced collaboration between law enforcement agencies and the private sector. This improvement is due, in part, to the Convention mandating that Parties establish domestic legal frameworks with provisions for collaborating with private entities.
8. **Technical Assistance**: The T-CY places a priority on providing technical support to states seeking to join the Budapest Convention. This support aims to streamline the Convention's full implementation and en-

hancing countries' international cooperation capabilities[9].

As of February 2020, the Budapest Convention had a significant and diverse influence, triggering extensive reforms in national legislation concerning cybercrime and electronic evidence worldwide:

- **Global Legislative Reforms:** 177 States (92%) globally were either in the process of updating their legislation or had recently completed reforms, with a substantial number drawing on the Budapest Convention as a reference or foundation for their revisions.
- **Harmonization of Laws:** The Convention has inspired 153 UN member States (79%) to incorporate its provisions into their legislative reforms, resulting in a harmonization of cybercrime laws across various jurisdictions.
- **Specific Criminal Provisions:** Roughly 106 States (55%) have implemented specific domestic provisions that align closely with the substantive criminal law articles of the Budapest Convention.
- **Procedural Law Enhancements:** The Convention has prompted 82 States (42%) to enact particular procedural authorities for investigating cybercrime and securing electronic evidence, mirroring Articles 16 to 21 of the Convention[9].

Some instances of how the Convention has impacted the modification of domestic laws include:

- **Mauritius (2003)** - Computer Misuse Act.
- **Romania (2003)** - Law 161/2003 - Prevention and combating cybercrime.
- **France (2004)** - Law No. 2004-575 on the Confidence in the Digital Economy.
- **Slovakia (2005)** - Amended the Criminal Code and the Criminal Procedure Code to to fulfill the obligations of the Budapest Convention.

- **Dominican Republic (2007)** - Law No. 53-07 on Crimes and High Tech Crimes.
- **Sri Lanka (2007)** - Computer Crimes Act No. 24 of 2007.
- **Ghana (2008)** - Electronic Transactions Act 722.
- **Italy (2008)** - Introduced additional rules in accordance to the Budapest Convention.
- **Germany (2009)** - Amended its Penal Code.
- **Portugal (2009)** - Law 109/2009 on Cybercrime.
- **Finland (2011)** - Amended its Criminal Code.
- **Croatia (2013)** - Changed its Criminal and Criminal Procedures to become fully in line with the Budapest Convention.
- **Peru (2013)** - Updated its substantive cybercrime law.
- **Cabo Verde (2017)** - Law No. 8/IX/2017[9].

Currently, the Budapest Convention consists of 71 Parties, with 21 countries having signed or been invited to accede[51].

3.3 Tallinn Manual on the International Law Applicable to Cyber-Operations

The Tallinn Manual was crafted due to the growing significance of cyberwarfare and operations in modern conflicts. As cyber capabilities became more intertwined with military strategies and state affairs, a clearer understanding of how international law applies to these activities was needed. Per invitation of NATO CCD COE an international group of legal experts collaborated to create this manual, providing a comprehensive framework for interpreting and applying international law in cyber warfare contexts. It aimed to address the lack of legal guidance and offer a valuable resource for legal practitioners, scholars, and policymakers dealing with the legal complexities of cyber operations[60].

The Tallinn Manual is divided into three components - Introduction (offers insights into the manual's intent and range, as well as details the methodology employed during its development); Part I (explores the fundamental international law framework relevant to cyberwarfare, covering sovereignty, state accountability, and the use of force); Part II (focuses on applying international humanitarian law to cyberwarfare, addressing key areas including targeting, precautions, and the safeguarding of civilians and civilian infrastructure, and examines how the law of neutrality pertains to cyber operations in times of armed conflict) - and features 95 "black-letter rules" that regulate diverse aspects of cyberwarfare. Each rule is accompanied by extensive commentary that explains its legal basis, normative essence, and practical implications within the domain of cyberwarfare. Together, these black-letter rules offer a comprehensive framework for comprehending and implementing international law in cyber warfare contexts. These rules are categorized under the following parts and titles:

I. Introduction

II. Part I - International cyber security law

   (a) States and cyberspace

   (b) The use of force

III. Part II - The law of cyber armed conflict

   (c) The law of armed conflict generally

   (d) Conduct of hostilities

   (e) Certain persons, objects, activities

   (f) Occupation

   (g) Neutrality[60]

Following its original publication in 2013, the group of 'Experts' published a new version in 2017 adopting new rules and complementing the previous work creating the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* also known as *Tallinn Manual 2.0*[59].

Tallinn Manual 2.0 addresses the changing landscape of cyber operations and to provide more extensive guidance on applying international law to cyber activities. The original Tallinn Manual primarily focused on the application of international law to cyber warfare during armed conflict. However, the manual's scope broadened due to the increasing relevance of cyber operations in times of peace and the escalating complexity of cyber threats, thereby covering legal frameworks beyond armed conflict. As such, instead of three components, the Manual now has five:[59]

I. Introduction

II. Part I - General international law and cyberspace

   (a) Sovereignty

   (b) Due diligence

   (c) Jurisdiction

   (d) Law of international responsibility

   (e) Cyber operations not *per se* regulated by international law

III. Part II - Specialized regimes of international law and cyberspace

   (f) International human rights

   (g) Diplomatic and consular law

   (h) Law of the sea

   (i) Air law

   (j) Space law

   (k) International telecommunication law

IV. Part III - International peace and security and cyber activities

   (l) Peaceful settlement

   (m) Prohibition of intervention

   (n) The use of force

   (o) Collective Security

V. Part IV - The law of armed conflict

(p) The law of armed conflict generally

(q) Conduct of hostilities

(r) Certain persons, objects, and activities

(s) Occupation

(t) Neutrality

Apart from alterations in the Manual's sectioning, the quantity of rules expanded from the initial 95 to 154[59].

Rule number in the first edition	Rule number in the current edition
Rule 1 – Sovereignty	On this issue, new Rules 1–4
Rule 2 – Jurisdiction	On this issue, new Rules 8–13
Rule 3 – Jurisdiction of flag States and States of registration	On this issue, new Rules 8–13
Rule 4 – Sovereign immunity and inviolability	Rule 5
Rule 5 – Control of cyber infrastructure	On this issue, new Rules 6–7
Rule 6 – Legal responsibility of States	On this issue, new Rules 14–30
Rule 7 – Cyber operations launched from governmental cyber infrastructure	N/A
Rule 8 – Cyber operations routed through a State	N/A
Rule 9 – Countermeasures	On this issue, new Rules 20–25
Rule 10 – Prohibition of threat or use of force	Rule 68
Rule 11 – Definition of use of force	Rule 69
Rule 12 – Definition of threat of force	Rule 70
Rule 13 – Self-defence against armed attack	Rule 71
Rule 14 – Necessity and proportionality	Rule 72
Rule 15 – Imminence and immediacy	Rule 73
Rule 16 – Collective self-defence	Rule 74
Rule 17 – Reporting measures of self-defence	Rule 75
Rule 18 – United Nations Security Council	Rule 76
Rule 19 – Regional organisations	Rule 77
Rule 20 – Applicability of the law of armed conflict	Rule 80
Rule 21 – Geographical limitations	Rule 81
Rule 22 – Characterisation as international armed conflict	Rule 82

Figure 3.1: Table of Concordance of Rules between Tallinn Manual and Tallinn Manual 2.0 (Part 1)[59]

.

Rule number in the first edition	Rule number in the current edition
Rule 23 – Characterisation as non-international armed conflict	Rule 83
Rule 24 – Criminal responsibility of commanders and superiors	Rule 85
Rule 25 – Participation generally	Rule 86
Rule 26 – Members of the armed forces	Rule 87
Rule 27 – *Levée en masse*	Rule 88
Rule 28 – Mercenaries	Rule 90
Rule 29 – Civilians	Rule 91
Rule 30 – Definition of cyber attack	Rule 92
Rule 31 – Distinction	Rule 93
Rule 32 – Prohibition on attacking civilians	Rule 94
Rule 33 – Doubt as to status of persons	Rule 95
Rule 34 – Persons as lawful objects of attack	Rule 96
Rule 35 – Civilian direct participants in hostilities	Rule 97
Rule 36 – Terror attacks	Rule 98
Rule 37 – Prohibition on attacking civilian objects	Rule 99
Rule 38 – Civilian objects and military objectives	Rule 100
Rule 39 – Objects used for civilian and military purposes	Rule 101
Rule 40 – Doubt as to status of objects	Rule 102
Rule 41 – Definitions of means and methods of warfare	Rule 103
Rule 42 – Superfluous injury or unnecessary suffering	Rule 104
Rule 43 – Indiscriminate means or methods	Rule 105
Rule 44 – Cyber booby traps	Rule 106
Rule 45 – Starvation	Rule 107
Rule 46 – Belligerent reprisals	Rule 108
Rule 47 – Reprisals under Additional Protocol I	Rule 109
Rule 48 – Weapons review	Rule 110
Rule 49 – Indiscriminate attacks	Rule 111
Rule 50 – Clearly separated and distinct military objectives	Rule 112
Rule 51 – Proportionality	Rule 113

Figure 3.2: Table of Concordance of Rules between Tallinn Manual and Tallinn Manual 2.0 (Part 2)[59]

.

Rule number in the first edition	Rule number in the current edition
Rule 52 – Constant care	Rule 114
Rule 53 – Verification of targets	Rule 115
Rule 54 – Choice of means or methods	Rule 116
Rule 55 – Precautions as to proportionality	Rule 117
Rule 56 – Choice of targets	Rule 118
Rule 57 – Cancellation or suspension of attack	Rule 119
Rule 58 – Warnings	Rule 120
Rule 59 – Precautions against the effects of cyber attacks	Rule 121
Rule 60 – Perfidy	Rule 122
Rule 61 – Ruses	Rule 123
Rule 62 – Improper use of the protective indicators	Rule 124
Rule 63 – Improper use of United Nations emblem	Rule 125
Rule 64 – Improper use of enemy indicators	Rule 126
Rule 65 – Improper use of neutral indicators	Rule 127
Rule 66 – Cyber espionage	Rule 89 – Spies
Rule 67 – Maintenance and enforcement of blockade	Rule 128
Rule 68 – Effect of blockade on neutral activities	Rule 129
Rule 69 – Zones	Rule 130
Rule 70 – Medical and religious personnel, medical units and transports	Rule 131
Rule 71 – Medical computers, computer networks, and data	Rule 132
Rule 72 – Identification	Rule 133
Rule 73 – Loss of protection and warnings	Rule 134
Rule 74 – United Nations personnel, installations, materiel, units, and vehicles	Rule 79
Rule 75 – Protection of detained persons	Rule 135
Rule 76 – Correspondence of detained persons	Rule 136
Rule 77 – Compelled participation in military activities	Rule 137
Rule 78 – Protection of children	Rule 138

Figure 3.3: Table of Concordance of Rules between Tallinn Manual and Tallinn Manual 2.0 (Part 3).[59]

Rule number in the first edition	Rule number in the current edition
Rule 79 – Protection of journalists	Rule 139
Rule 80 – Duty of care during attacks on dams, dykes, and nuclear electrical generating stations	Rule 140
Rule 81 – Protections of objects indispensable to survival	Rule 141
Rule 82 – Respect and protection of cultural property	Rule 142
Rule 83 – Protection of the natural environment	Rule 143
Rule 84 – Protection of diplomatic archives and communications	On this issue, new Rules 39–42
Rule 85 – Collective punishment	Rule 144
Rule 86 – Humanitarian assistance	Rule 145
Rule 87 – Respect for protected persons in occupied territory	Rule 146
Rule 88 – Public order and safety in occupied territory	Rule 147
Rule 89 – Security of the Occupying Power	Rule 148
Rule 90 – Confiscation and requisition of property	Rule 149
Rule 91 – Protection of neutral cyber infrastructure	Rule 150
Rule 92 – Cyber operations in neutral territory	Rule 151
Rule 93 – Neutral obligations	Rule 152
Rule 94 – Response by parties to the conflict to violations	Rule 153
Rule 95 – Neutrality and Security Council actions	Rule 154

Figure 3.4: Table of Concordance of Rules between Tallinn Manual and Tallinn Manual 2.0 (Part 4)[59]

.

It is essential to recognize that both The Tallinn Manual and Tallinn Manual 2.0 are not legally binding documents and do not possess the authority of international law. They serve as scholarly resources offering expert analysis and interpretations of how current international law pertains to cyber operations.

While widely respected in the international legal community, the interpretations and recommendations presented in the manuals do not carry legal enforcement. Nevertheless, they are valuable tools for policymakers, legal experts, and scholars seeking to comprehend the legal consequences of cyber operations within the existing international law framework. The primary legal authority in international law remains with treaties, customary international law, and the decisions made by international courts and tribunals[60][59]. It is to be expected an updated version of the Tallinn Manual to be launched soon, as Tallinn Manual 3.0 is now in the works[67].

Chapter 4

Discussion

The notion of War is dynamic and has evolved since before General Sun Tzu's time (5th century BC). It is set to adapt alongside societal changes, community advancements, globalization driven by technological progress, and changing perspectives on the world. Once a matter of life and death, war has transformed into a "political game" that can be orchestrated from the comfort of our homes. With just a computer, one can initiate a conflict, whether confined to cyberspace (Estonia, 2007) or capable of impacting the physical world through the cyber domain (Stuxnet, 2010), or supporting a physical conflict through an alternate battleground - *cyberspace* (Georgia, 2008).

To date, no countries have established specific laws or regulations pertaining to cyberwarfare, and this absence extends to the international level as well. There are laws on cybercrime and on war, but not on cyberwar.

The Convention on Cybercrime sets forth procedural laws for electronic evidence gathering, encourages international cooperation among signing states, and upholds human rights and freedoms. While these laws pertain to cybercrime, the strides in international legislation are commendable and have shown effectiveness. This Convention particularly addresses a critical aspect of cyber offenses - the ever-evolving nature of the cyber domain. To tackle these changes, T-CY convenes plenary sessions biannually for in-depth discussions.

Following the 2007 cyber attacks on Estonia, the legal response primarily cat-

egorized the events as cyber crimes under Estonian law, steering away from labeling them as acts of warfare or terrorism. Challenges arose in identifying perpetrators within legal constraints set by the Estonian Surveillance Act, which limited surveillance to authorized agencies. While NATO's Article 5[1] was not invoked due to cyber attacks not being defined as direct military actions, Estonia pursued international cooperation, seeking assistance under mutual legal agreements. However, the intricate global nature of the attacks complicated identifying culprits within national legal systems. Consequently, Estonia broadened criminal law provisions, implementing a Cyber Security Strategy and amending the Penal Code to encompass cyber crimes, including those driven by terrorist motives[69].

The 2008 cyber attacks targeting Georgia spurred legal discussions on the interpretation of the Law of Armed Conflict (LOAC), criminal law, and regulations within the Information and Communication Technology (ICT) industry. Deliberations centered on whether the attacks could be classified as "cyber warfare" under LOAC, given uncertainties around state involvement and the limited impact on Georgian civilians. As LOAC proved intricate to apply, the focus shifted towards criminal law, emphasizing the importance of robust ICT legal frameworks and international cooperation. Concerns emerged over the neutrality of international aid provided to Georgia, although it was considered lawful as it did not violate neutrality principles.[69]

The Stuxnet incident entailed a complex computer worm that aimed at disrupting Iranian nuclear facilities by manipulating industrial control systems. This breach blurred the boundaries between physical and cyber realms, posing challenges in determining suitable penalties for the actions taken in this attack. Dr. Katharina Ziolkowski's analysis of the Stuxnet incident delves into several legal aspects:

[1] Article 5 - "The Parties agree that an armed attack against one or more of them [...] shall be considered an attack against them all [...], if such an armed attack occurs, each of them, [...], will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."[65]

1. **Use of Force**: The examination determines if deploying Stuxnet qualifies as a use of force under Article 2(4) of the UN Charter[2], considering severity, immediacy, and direct consequences.
2. **Self-Defense**: The concept of pre-emptive self-defense is discussed in relation to possessing nuclear weapons, clarifying that possession alone does not constitute an imminent attack.
3. **Countermeasures**: The assessment explores whether Stuxnet could be viewed as a legal countermeasure, requiring a response to a prior wrongful act.
4. **Economic Coercion and Non-Intervention**: The paper addresses economic coercion and non-intervention, highlighting when coercion breaches a state's internal affairs.
5. **Legality**: The analysis suggests that if Stuxnet caused no physical harm and was state-controlled, it might not breach international law, possibly being seen as a lawful action[73].

These examples highlight the crucial and pressing need for the establishment of cyberwar laws. If there had been legislation addressing cyberwarfare, the legal processes and outcomes in these three cases could have diverged significantly.

There have been initiatives towards legislation, exemplified by the Tallinn Manual. The first version was issued in 2013, followed by Tallinn Manual 2.0 in 2017, with Tallinn Manual 3.0 currently in progress. These manuals are predominantly seen as references and sources of inspiration for legal practitioners, scholars, and policymakers, rather than definitive tools for cyberwar legislation. The Budapest Convention has proven that international cooperative efforts can effectively deter cybercrime. *Why not in legislating cyberwar and applying the principles of war as well?*

[2] Article 2(4) - "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[6]

Chapter 5

Conclusions

Initially focusing on keywords like Cyberwar, Cybercrime, Cyberlaws, and Laws of War, this dissertation found fragmented information, leading to challenges in establishing a precise methodology. Consequently, the strategy encompassed exploring official websites concerning domestic and international laws, like the ICRC and the CoE databases, and referencing publications from sources such as the NATO CCD COE library and other official government websites.

This thesis diverges from compartmentalized alignment, opting for a comprehensive approach to the initial theme. It integrates examples with laws and utilizes existing treaties to illustrate occurrences, enabling an understanding of the evolution timeline of concepts, country involvement, legislative initiatives, and international cooperation in seeking consensus on cyberwar.

The absence of specific legislation and regulations to address cyberwarfare leads to criminal actions that could constitute acts of war being categorized simply as cybercrimes and punished accordingly, without considering the warfare aspect.

To address this legislative gap, it would be compelling to establish an international task force not only to tackle this issue but also to establish internationally accepted regulations on cyberwarfare.

Furthermore, close to cyberwarfare lies the concept of cyber defense. It would

be insightful to examine nations' readiness to combat cyber threats and the defensive measures they have implemented.

References

[1] *Additional Articles relating to the Condition of the Wounded in War. Geneva, 20 October 1868.* `https://ihl-databases.icrc.org/en/ihl-treaties/add-arts-gc-1868?activeTab=historical`. Accessed: 2023-12-12.

[2] Marwan Albahar. "Cyber attacks and terrorism: a twenty-first century conundrum". In: vol. 25. 4. Springer, 2019, pp. 993–1006.

[3] Col. Patrick D. Allen and Lt. Col. Chris Demchack. *The Palestinian-Israeli Cyberwar*. Militarry Review, 2003.

[4] Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser. "Binary bullets: the ethics of cyberwarfare". In: Oxford University Press, 2016.

[5] John Arquilla and David Ronfeldt. "Cyberwar is coming!" In: *Comparative Strategy* 12.2 (1993), pp. 141–165.

[6] UN Charter. "Charter of the United Nations". In: *June* 26 (1945), p. 59.

[7] Eric Chien, Liam OMurchu, and Nicolas Falliere. "{W32. Duqu}: The Precursor to the Next Stuxnet". In: *5th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET 12)*. 2012.

[8] *command-and-control server (CC server)*. `https://www.techtarget.com/whatis/definition/command-and-control-server-CC-server`. Accessed: 2024-04-20.

[9] Cybercrime Convention Committee et al. "The Budapest Convention on Cybercrime: benefits and impact in practice". In: *France: Council of Europe* (2020).

[10] *Computer Fraud and Abuse Act (CFAA).* https://www.nacdl.org/Landing/ComputerFraudandAbuseAct. Accessed: 2024-04-21.

[11] *Convention (III) for the Adaptation to Maritime Warfare of the Principles of the Geneva Convention of 22 August 1864. The Hague, 29 July 1899.* https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iii-1899?activeTab=historical. Accessed: 2023-12-12.

[12] *Convention (X) for the Adaptation to Maritime Warfare of the Principles of the Geneva Convention. The Hague, 18 October 1907.* https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-x-1907?activeTab=historical. Accessed: 2023-12-12.

[13] *Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field. Geneva, 27 July 1929.* https://ihl-databases.icrc.org/en/ihl-treaties/gc-wounded-1929?activeTab=historical. Accessed: 2024-01-20.

[14] *Convention for the Amelioration of the Condition of the Wounded in Armies in the Field. Geneva, 22 August 1864.* https://ihl-databases.icrc.org/en/ihl-treaties/gc-1864?activeTab=historical. Accessed: 2023-12-12.

[15] *Convention relative to the Treatment of Prisoners of War. Geneva, 27 July 1929.* https://ihl-databases.icrc.org/en/ihl-treaties/gc-pow-1929?activeTab=historical. Accessed: 2024-01-20.

[16] Council of Europe. *Convention on Cybercrime (ETS No. 185).* 2001.

[17] Marco De Falco. "Stuxnet facts report: A technical and strategic analysis". In: *NATO CCDCOE.* (2012).

[18] *Declaration (IV,1), to Prohibit, for the Term of Five Years, the Launching of Projectiles and Explosives from Balloons, and Other Methods of Similar Nature. The Hague, 29 July 1899.* https://ihl-databases.icrc.org/en/ihl-treaties/hague-decl-iv-1-1899?activeTab=historical. Accessed: 2023-12-12.

[19] *Declaration concerning the Laws of Naval War. London, 26 February 1909.* https://ihl-databases.icrc.org/en/ihl-treaties/london-decl-1909?activeTab=historical. Accessed: 2023-12-12.

[20] Dorothy E Denning. "Activism, Hacktivism, and Cyberterrorism: The Internet as". In: (2001).

[21] Attorney-General's Department. "Cybercrime Act 2001". In: *Office of Legislative Drafting, Attorney-General's Department, Canberra* (1990).

[22] J Di Maggio. "The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organised Cybercrime". In: Harper Collins, New York, NY, 2022.

[23] Charles Doyle. "Cybercrime: an overview of the federal computer fraud and abuse statute and related federal criminal laws". In: (2011).

[24] *Draft International Convention on the Condition and Protection of Civilians of enemy nationality who are on territory belonging to or occupied by a belligerent. Tokyo, 1934.* https://ihl-databases.icrc.org/en/ihl-treaties/tokyo-draft-conv-1934?activeTab=historical. Accessed: 2024-01-21.

[25] Roman Dremliuga, Olga Dremliuga, and Pavel Kuznetsov. "Combating the Threats of Cybercrimes in Russia: Evolution of the Cybercrime Laws and Social Concern". In: *Communist and post-communist studies* 53.3 (2020), pp. 123–136.

[26] Institut de Droit International. *Manuel des lois de la guerre maritime dans les rapports entre belligérants.* Institut de Droit International, 1913. URL: https://www.idi-iil.org/en/sessions/oxford-1913/?post_type=publication.

[27] Institut de Droit International. *Manuel des lois de la guerre sur terre.* Institut de Droit International, 1880. URL: https://www.idi-iil.org/en/sessions/oxford-1880/?post_type=publication.

[28] Council of Europe. *Additional protocol to the convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems: Strasbourg, 28. 1. 2003*. Council of Europe Publ., 2003.

[29] Council of Europe. *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*. Council of Europe Publ., 2021.

[30] *Final Act of the Diplomatic Conference of Geneva, 12 August 1949*. https://ihl-databases.icrc.org/en/ihl-treaties/geneva-finact-1949. Accessed: 2024-01-21.

[31] *Final Act of the Diplomatic Conference. Geneva, 27 July 1929*. https://ihl-databases.icrc.org/en/ihl-treaties/geneva-finact-1929?activeTab=historical. Accessed: 2024-01-20.

[32] *First draft Convention adopted in Monaco (Sanitary cities and localities), 27 July 1934*. ://ihl-databases.icrc.org/en/ihl-treaties/monaco-draft-conv-1934?activeTab=historical.

[33] Kenneth Geers. "Cyberspace and the changing nature of warfare". In: *SC magazine* 27 (2008).

[34] *Geneva Conventions of 1949, Additional Protocols and their Commentaries*. https://ihl-databases.icrc.org/en/ihl-treaties/geneva-conventions-1949additional-protocols-and-their-commentaries. Accessed: 2024-01-22.

[35] Lionel Giles et al. *Sun Tzu on the art of war*. Kegan Paul Kegan Paul, 2002.

[36] H. Grotius and R. Tuck. *The Rights of War and Peace*. Major legal and political works of Hugo Grotius bk. 1. Liberty Fund, 2005. ISBN: 9780865974371. URL: https://books.google.pt/books?id=t8S1mQEACAAJ.

[37] H. Grotius and M.J. Van Ittersum. *Commentary on the Law of Prize and Booty*. Major legal and political works of Hugo Grotius. Liberty Fund, 2006. ISBN: 9780865974746. URL: https://books.google.pt/books?id=9CUiAQAAIAAJ.

[38] Monique Hébert and Marilyn Pilon. *Computer crime*. Vol. 87. Library of Parliament, Research Branch, 1991.

[39] *History of the United Nations*. https://www.un.org/en/about-us/history-of-the-un. Accessed: 2024-01-21.

[40] *Instructions for the Government of Armies of the United States in the Field (Lieber Code). 24 April 1863.* https://ihl-databases.icrc.org/en/ihl-treaties/liebercode-1863?activeTab=historical. Accessed: 2023-12-12.

[41] James Kurose and Keith Ross. "Computer networks: A top down approach featuring the internet". In: *Peorsoim Addison Wesley* (2010).

[42] *Law of the Hague*. https://casebook.icrc.org/a_to_z/glossary/law-hague. Accessed: 2023-12-12.

[43] *Milestones in UN History 1941-1950*. https://www.un.org/en/about-us/history-of-the-un/1941-1950. Accessed: 2024-01-21.

[44] Minister of Justice of Canada. *Criminal Code of Canada, R.S.C., 1985, c. C-46*. Section 342.1. 1985.

[45] *MITRE ATTCK*. https://attack.mitre.org/software/S0143/. Accessed: 2024-09-27.

[46] Takato Natsui. "Cybercrimes in Japan: Recent Cases, Legislations, Problems and Perspectives". In: *Meiji University* (2003), pp. 1–22.

[47] Jens David Ohlin, Kevin Govern, and Claire Finkelstein. *Cyber war: law and ethics for virtual conflicts*. OUP Oxford, 2015.

[48] Brian Orend. "War". In: *Stanford Encyclopedia of Philosophy*. 2008.

[49] Rain Ottis. "Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective". In: *Proceedings of the 7th European Conference on Information Warfare*. Academic Publishing Limited Reading, MA. 2008, p. 163.

[50] UK Parliament. "Computer Misuse Act 1990". In: *Queen's Printer of Acts of Parliament: London* (1990).

[51] *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY.* `https://www.coe.int/en/web/cybercrime/parties-observers`. Accessed: 2024-04-25.

[52] Yong Pi. "New china criminal legislations in the progress of harmonization of criminal legislation against cybercrime". In: *Retrieved December* 12 (2011), p. 2017.

[53] Isaac R Porche III. "Cyberwarfare: An Introduction to Information-Age Conflict". In: Artech House, 2019.

[54] *Project of an International Declaration concerning the Laws and Customs of War. Brussels, 27 August 1874.* `https://ihl-databases.icrc.org/en/ihl-treaties/brussels-decl-1874?activeTab=historical`. Accessed: 2023-12-12.

[55] Filip Radoniewicz. "Cyberspace, Cybercrime, Cyberterrorism". In: *Cybersecurity in Poland* (2022), p. 33.

[56] Law Revision Commission of the Republic of Singapore. "Computer Misuse Act (Chapter 50A)". In: *The Statutes of the Republic of Singapore* (1993).

[57] *Resolutions of the Geneva International Conference. Geneva, 26-29 October 1863.* `https://ihl-databases.icrc.org/en/ihl-treaties/geneva-res-1863?activeTab=historical`. Accessed: 2023-12-12.

[58] *Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare. Drafted by a Commission of Jurists at the Hague, December 1922 - February 1923.* `https://ihl-databases.icrc.org/en/`

ihl-treaties/hague-rules-1923?activeTab=historical. Accessed: 2024-01-20.

[59] M.N. Schmitt and NATO Cooperative Cyber Defence Centre of Excellence. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations". In: Cambridge University Press, 2017. ISBN: 9781107177222. URL: https://books.google.pt/books?id=n9wcDgAAQBAJ.

[60] Michael N Schmitt. "Tallinn manual on the international law applicable to cyber warfare". In: Cambridge University Press, 2013.

[61] Jeremy Straub and Terry Traylor. "Introduction of a maritime model for cyber and information warfare". In: *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE. 2018, pp. 25–29.

[62] Francisco Suárez and Thomas Pink. *Selections from three Works*. Liberty Fund, 2014.

[63] SA TEAM. "sKyWIper (aka Flame aka Flamer): A complex malware for targeted attacks". In: *Budapest, Hungary: Laboratory of Cryptography and System Security (CrySyS Lab)* (2012).

[64] *The Laws of War on Land. Oxford, 9 September 1880*. https://ihl-databases.icrc.org/en/ihl-treaties/oxford-manual-1880. Accessed: 2023-11-09.

[65] *The North Atlantic Treaty*. https://www.nato.int/cps/en/natohq/official_texts_17120.htm. Accessed: 2024-05-05.

[66] *The San Francisco Conference*. https://www.un.org/en/about-us/history-of-the-un/san-francisco-conference. Accessed: 2024-01-21.

[67] *The Tallinn Manual*. https://ccdcoe.org/research/tallinn-manual/. Accessed: 2024-01-22.

[68] Catherine A Theohary and John W Rollins. *Cyberwarfare and cyberterrorism: In brief*. Congressional Research Service Washington, DC, 2015.

[69] Eneken Tikk, Kadri Kaska, and Liis Vihul. *International cyber incidents: Legal considerations*. Cooperative Cyber Defence of Excellence (CCD COE), 2010.

[70] Joseph B Tompkins Jr and Linda A Mar. "The 1984 Federal Computer Crime Statute: a partial answer to a pervasive problem". In: *Computer/LJ* 6 (1985), p. 459.

[71] *Treaty relating to the Use of Submarines and Noxious Gases in Warfare. Washington, 6 February 1922.* `https://ihl-databases.icrc.org/en/ihl-treaties/washington-treaty-1922?activeTab=historical`. Accessed: 2024-01-13.

[72] *What is DNS?* `https://www.cloudflare.com/learning/dns/what-is-dns/`. Accessed: 2024-04-20.

[73] Katharina Ziolkowski. *Stuxnet - Legal Considerations*. NATO Cooperative Cyber Defence Centre of Excellence. Draft document. Tallinn, Estonia, 2012. URL: `https://ccdcoe.org/research.html`.