Cybersecurity under International Law

Dr. Habib Badawi – Lebanese University

(habib.badawi@ul.edu.lb – habib.badawi@gmail.com)

https://orcid.org/0000-0002-6452-8379

ABSTRACT

As the twenty-first century has progressed, conventional and nuclear weapons have changed, and neither can be decisive for victory. Instead, advancing technologies have become a dangerous high-tech weapon in the digital age we live in, known as "cyber warfare". Compared to conventional weapons, this armament is more lethal in terms of destroying the internal systems of an opponent.

Cyberwarfare is the use of digital attacks to attack the assets of a state or entity, causing physical damage like what happens in an actual war. Cyberattacks may take the form of a practical weapon by disrupting radar installations and air defense systems, deranging oil pipeline flow systems, or crippling the software of its nuclear plants, causing the enemy's defense strategy to collapse. On the home front, "information warfare" plays a key role in shattering society's morale, declining immunity.

The importance of this study stems from its legal approach and its attempt to briefly present aspects of "cyber operations" while resorting to international texts to present the principles that are supposed to govern this type of hidden warfare.

Based on the main axes of the study, the following questions are addressed regarding the concept of "cyber warfare":

1. How does cyber-online espionage work?
2. What are the challenges under the Cyber Operations Act?
3. Cyberattacks take many forms, but which ones are the most dangerous?

In this study, methods of cybersecurity were accurately presented and relationships between variables were examined using analysis and objectivity. The analytical-deductive approach was used to determine the general rules of international humanitarian law.

This study utilizes an interdisciplinary approach that combines legal analysis, policy research, and military strategy. The research methodology includes a systematic review of relevant literature, a review of existing international and domestic laws governing cyber warfare, and a comparative analysis of the cyber defense capabilities of different countries. Additionally, this study also considers the implications of the use of cyber weapons and the need for a legal framework to govern their use. Finally, the research includes an analysis of the Cyber Operations Act and the implications of this Act for cyber operations and cyber espionage.

KEYWORDS

Cybersecurity, International Law, Cyber Warfare, Cyber Operations, Cyber Espionage, Cyber Defense.

Introduction

The purpose of this study is to highlight the implications of cyberlaw for military operations. It also aims to translate academic and theoretical discussions into concrete legal advice. In addition, it analyzes recent cyberspace operations under the legal system applicable to weapons, means of war, and their methods. An assessment that focuses on how to use cyber capability, particularly the primary objective of its use, is more accurate in determining what it is (weapons or not) and conforms to international law more effectively and objectively.

Since the beginning of the twenty-first century, warfare has changed, and conventional weapons, as well as nuclear weapons, are no longer decisive for victory. Instead, advancing technologies represent a dangerous high-tech weapon in the digital era we live in, known as "cyber warfare". In comparison to conventional weapons, this armament is more lethal in terms of destroying an opponent's internal system.

There are many difficulties in determining the party executing cyberattacks, including the absence of visual evidence and the difficulty of accessing the evidence to inform the perpetrator of his crime with means of technical protection, such as the perpetrator's use of passwords in a way that prevents access to electronic evidence or his encryption of information.

The importance of this study stems from its legal approach and its attempt to briefly present aspects of "cyber operations" while resorting to international texts to present the principles that are supposed to govern this type of hidden warfare, especially the "Tallinn Manual" issued by the North Atlantic Treaty Organization (NATO).

The main objective of this study is to shed light on the impact of cybersecurity laws on military operations. It also aims to translate academic and theoretical discussions into concrete legal advice. Based on that, examples of modern cyber capabilities and operations are presented, highlighting the issues involved in cyberspace operations for analysis under the law. The assessment focuses on how countries, groups, and individuals use cyber capabilities and the legality of their use of those capabilities.

National security, public safety, and the global economy depend on the immunity of the nation-state and the international community in cyberspace. Therefore, the world's leading countries must be fully prepared to confront "cyber warfare," which is the greatest threat to global stability. It is dangerous to conduct cyberattacks as part of cyberwarfare methods and destructive methods, as well as to conduct "information warfare" to discover the strengths and weaknesses of your enemies, friends, and neutrals alike.

A major challenge in the modern era is the problem of cyberattacks. It is expected that the information security systems of sovereign countries will suffer from a process of overlap and discord. There is a particular fear of structural imbalance among those involved in the defense system, communication units, and economic insurance.

Hence, protecting the country's cyberspace and preparing for all possible cyberattack scenarios is imperative. Using networks, big data, technology, virtualization, cloud computing, cloud services, cryptocurrencies, widespread deployment, legacy systems, and the integration of cyber systems with physical systems, cyberspace is where these processes are carried out.

As part of this study, the methods of cybersecurity were presented accurately, and the relationships between variables were investigated while relying on analysis and objectivity in collecting information. In order to determine the general rules of international humanitarian law, the analytical-deductive approach was used.

The findings of this study show that cyber law and its implications for military operations must be taken into consideration. Cyberlaw is an essential component of modern warfare and provides a legal framework for the use of cyberspace operations that may have far-reaching implications. The study also emphasizes the importance of international law in regulating cyber activities. It stresses the need for countries to develop their legal frameworks

to address issues such as digital security, privacy, surveillance, and the use of force.

In addition, the study highlights the importance of developing comprehensive strategies to counter cyber threats. In addition, the study emphasizes the need for increased bilateral cooperation to prevent the proliferation of cyber weapons and malicious cyber activities. Finally, the study recommends the adoption of measures to ensure the protection of civilians and non-combatants in cyberspace operations and to ensure that international humanitarian law is observed in such operations.

1. Cyberespionage

Cyberespionage is a form of cyberattack that aims to steal confidential, sensitive, or intellectual property data to gain an advantage over a rival government company or entity. Espionage is " the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company" (Merriam-Webster, 2022).

In the world of the Internet, spies are armies of infiltrators from all over the world. These infiltrators use war and electronics as a means of economic, political, or military gain. These high-value cybercriminals have the knowledge and technical capacity to penetrate government infrastructure, financial and real estate systems, or utility resources such as airports, ports, etc. They have been able to influence the outcome of political elections in several countries. The United States accuses Russia of interfering in the election results that led to Trump's victory by creating international chaos, and helping companies succeed or fail (Justice & Bricker, 2019). Many of these attackers use Advanced Persistent Threats as modus to sneak into corporate and state networks or systems and stay undetected for years (Lee, 2017).

Figure1- APT Security Measures (Imperva, 2022)

In Hague Convention of 1907 (ICRC, Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 1907), Article 29 "*A person can only be considered a spy when, acting clandestinely or on false pretences, he obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party. Thus, soldiers not wearing a disguise who have penetrated into the zone of operations of the hostile army, for the purpose of obtaining information, are not considered spies. Similarly, the following are not considered spies: Soldiers and civilians, carrying out their mission openly, entrusted with the delivery of despatches intended either for their own army or for the enemy's army. To this class belong likewise persons sent in balloons for the purpose of carrying despatches and, generally, of maintaining communications between the different parts of an army or a territory"* (ICRC, Annex to the Convention: Regulations respecting the laws and customs of war on land - Section II: Hostilities - Chapter II: Spies - Regulations: Art. 29, 1907). The law clearly states that an individual can only be considered a spy for a particular state if he or she obtains information in the enemy's area of operations by acting secretly and intending to inform the hostile party. Therefore, undetected soldiers who enter the area of operations of an army hostile to obtain military or intelligence information are

not considered spies, nor are spies of soldiers or civilians of a particular state who carry out their duties in public or are mandated to deliver letters addressed either to their army or to the enemy army.

As stipulated in Article 46 (2) of the First Additional Protocol of 1977 to the Geneva Convention, it may not engage in espionage if it is conducted by the armed forces of a party to a particular conflict and on instruction from that party (I, 1977). Adversary-controlled territory used to collect information or attempt to collect it in the uniform of its country's armed forces is considered part of this convention (ICRC, 1977).

Cyberespionage is a major security concern in the modern world. Governments, organizations, and individuals are the targets of a range of cyber-espionage activities. Cyber spies can steal data and intellectual property, disrupt business operations, and even influence political outcomes. To protect against digital espionage, organizations and individuals should take proactive measures to protect their networks and data. This includes regularly patching systems, using strong passwords, encrypting data, and monitoring network activity for suspicious activity. Additionally, organizations should consider investing in security solutions such as firewalls, intrusion detection/prevention systems, and anti-malware software.

The purpose of cyberespionage is to steal confidential, sensitive, or intellectual property data from a competing government agency or company. Espionage is "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company" (Merriam-Webster, 2022). Cyberespionage is a major security concern in the modern world. Governments, organizations, and individuals are the targets of a range of cyber-espionage activities. Using cyberspace, spies can steal data and intellectual property, disrupt business operations, and even influence political outcomes.

2. Cyber Operations

One of the first issues facing cyber operations is the distinction between them and espionage. There has been an unwritten agreement between countries to ignore espionage in international human rights law for many years but identifying cyber-actions that are espionage is a challenge due to the similarities between cyberespionage and cyberattacks on the ground. Internet experts and policymakers seem determined to exclude espionage from the same consideration as cyber operations (Bateman, 2022).

Cyberespionage and cyberattack techniques are often identical, and espionage is usually a necessary condition for an attack. There is only limited or no ability to distinguish between the electronic technologies used in espionage and those used in a cyberattack. In the latter case, once the opponent controls the computer, he can do what he wants with the piece of information (a type of spy), disable, or destroy the system.

Cyber espionage is not just copies of information from a system; it usually requires some form of electronic maneuvering that makes it possible to steal targeted information and may require action to prevent the system from accessing information. For example, a process can be carried out to weaken encryption or eliminate the electronic capability of the target. This will force it to use an alternative system that provides easier access to its database and decrypts it. Once the system is hacked, the new owner can take any action, including processing and stealing data. The victim cannot determine whether an unauthorized user intends to spy, disable, or destroy the system when such an action is taken (Crime, 2022).

The only difference between operations aimed at gathering intelligence (espionage) and those designed to cause electronic disruption or destruction is often the intention behind this action. The first is used to collect information in multiple ways, while the second is used to support operational planning or carry out conventional military operations. Some assistance is as direct as gathering information about the deployment of enemy forces or the strategic supplies they employ on the battlefield; other assistance is indirect, such as training partner armies or exchanging aid with friendly countries. Most support activities are not controversial from a legal perspective, although they may be conducted in secret within the state without their consent and are espionage-like (Prochko, 2018).

This division in cyber activities makes legal advice to military commanders more challenging than in conventional military operations. Cyberactivity is not controversial when the primary objective is to collect or access information. However, activity conducted for a purpose other than intelligence gathering can be defined as a weapon attack requiring a comprehensive analysis involving all branches of the state. The definition of an electronic weapon may provide a basis for objectively determining the nature of activities in cyberspace.

Cyber operations have the potential to revolutionize warfare, but legal definitions and considerations need to be established to protect against abuse. It is paramount to recognize the distinction between cyberespionage and cyberattacks, and to ensure that international laws are respected in cyberspace. Additionally, organizations and individuals should take proactive steps to protect their networks and data from cyberespionage. This includes regularly patching systems, using strong passwords, encrypting data, and monitoring network activity for suspicious activity. Organizations should consider investing in security solutions such as firewalls, intrusion detection/prevention systems, and anti-malware software.

3. Challenges under the Cyber Operations Act

The Pentagon defines cyberspace as a man-made field and considers its military operations to blend issues of geography, sovereignty, law, and civil rights in ways that extend beyond traditional legal boundaries and must be approached differently (Crowther, 2017).

Most legal analysts are comfortable discussing concepts of war in the areas of ground warfare, air warfare, or naval warfare. However, the common use of those concepts does not appear to have moved into cyberwarfare. Despite the widespread use of the term’s "war" and "attack" in an electronic context during military operations. For example, the term "cyber warfare" is used to describe the use of cyberspace and cyberattacks for military operations, ranging from cyberattacks against logistics sites to violent combat attacks (Haig, 2015).

Because of their nature, it may be difficult to classify cyber operations within the scope of military operations, and the fundamental question remains as to whether Article 51, which states: *“Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or*

restore international peace and security" (Nations, 2016).

Also, Article 2 (4), which states: *"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"* (Nations, Chapter I — Purposes and Principles, 2021)

The dilemma arises when both are violated. The international community continues to analyze cyber incidents on a case-by-case basis, focusing on whether an electronic activity constitutes a prohibited use of force under Article 2 (4) or an armed attack that would generate the right to exercise self-defense as stipulated in Article 51.

Exploit the Tallinn Manual (Badawi, 2022) and the cyberattack known as Stuxnet (Chen, 2014), a computer worm discovered in June 2010 that was specifically written to take over certain programmable industrial control systems and cause the equipment run by those systems to malfunction while feeding false data to the systems monitors, indicating the equipment was running as intended, as an example. It is easy to distinguish between electronic operations in parallel with an armed attack under Article 51 of the United Nations Charter. Those that do not correspond to an armed attack, and perhaps the most relevant question is whether these operations constitute a use of force under Article 2 (4) of the Charter of the United Nations.

The most complete analysis to determine the nature of cyber operations as an attack is a six-point test conducted by one of the researchers, Professor Schmidt, in which he tries to classify cases when the use of cyberspace is considered a use of force under Article 2 (4), which includes the elements of immediate, direct, invading, measurable, and legitimate risk. When applying these criteria to determine the legality of an attack, it considers the consequences of cyberattacks and assesses them as equal to conventionally armed attacks (Oona A. Hathaway, 2012).

A range of information technology operations does not amount to an armed attack. They are not considered the use of force under international law, nor can they be considered interference with the state's ability to exercise its sovereignty. Instead, they constitute a breach of peace, are coercive and unwelcome, and may be the subject of diplomatic objection and action by the UN Security Council. As a basis for legalizing cyber-military operations, it must be convinced that certain cyber-warfare activities are not cyberattacks, do not constitute acts of war, and comply with international law. This logic applies to cyberespionage, although when examining the actual techniques used, the distinction between them and electronic processes is not clear and poses a dilemma to consider.

Failure to accurately describe what is an electronic weapon and what is not an electronic weapon makes it more difficult to determine which states comply with international law and what they must do to ensure that their electronic activities comply with the law of war. A rational approach to cyberwarfare analysis helps clarify legal rules in a way that supports military operations in cyberspace. This includes an analysis of the mechanisms and techniques used in some cyber incidents, which highlights the difficulty of applying theoretical academic details to real cyber operations.

The Cyber Operations Act, passed by Congress in 2021, provides a legal framework for the US government to respond to cyberattacks by foreign actors. The Act provides the government with the authority to take defensive measures in response to malicious

cyber activity and to impose sanctions on those responsible for cyberattacks. However, several challenges must be addressed to effectively use the Act.

First, the Act does not provide clear guidance on when a cyberattack constitutes an "armed attack." This lack of clarity can create confusion for policymakers, as it is not always clear when a cyberattack warrants a response or sanctions under the Act. Second, the scope of the Act is limited to cyberattacks targeting US critical infrastructure, government agencies, and US companies. This means that other cyberattacks, such as those targeting individuals or foreign companies, are not covered by the Act. Additionally, the Act does not guide how to respond to cyber threats that are not considered to be an "armed attack" or how to respond to cyber threats that are directed at US allies. Third, the Act does not address the use of offensive cyber operations, such as offensive cyberattacks or cyber espionage. As such, the US government must rely on Executive Order 12333 and other legal frameworks.

4. Methods of Cyber Attack

Supervisory Control and Data Acquisition (SCADA) (Sampalli, 2020) systems are a control system architecture comprising computers, networked data communications, and graphical user interfaces for high-level supervision of machines and processes. It also covers sensors and other devices, such as programmable logic controllers, that interface with processing plants or machinery. SCADA is an essential area of national cyber-development, controlling and managing facilities, transportation, and manufacturing systems. Recognition of the threat to these systems has led the United States to establish the ICS-CERT cyber emergency response team under the supervision of the Department of Homeland Security to enhance the defense of these systems, since the details of any actual cyber operations classified as confidential are open-source, open-source electronic operations that can be inferred from how electronic capability can be used in a cyberattack.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) operates within the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share information about control systems-related security incidents and mitigation measures.

"Industrial Control Systems Cyber Emergency Response Team."

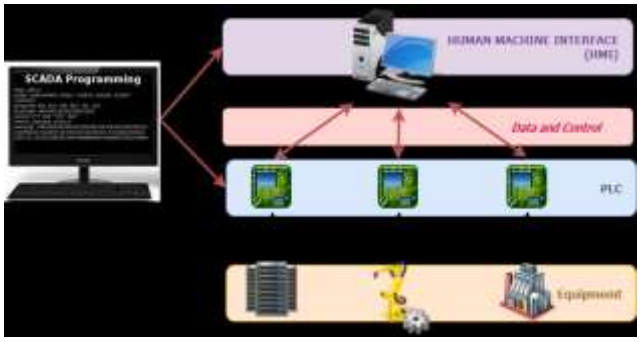

Figure2 - SCADA Diagram Example System with Main Components (How Do SCADA Systems Work?, 2022)

Stuxnet is sophisticated malicious computer code that aims to spread using autorun automation throughout the Web and is designed to be able to perform multiple functions. Once installed, it identifies the host system, develops host network maps, distributes copies of them, and reports what it has found.

In the Iranian case, software was inserted into the centrifuge's operating system to process

uranium. The malware accelerated or slowed down these supersonic devices, and these sudden speed changes disrupted them. In parallel, another component of the program caused Iran's electronic surveillance program to report that centrifuges were working properly. This prevented the problem from being detected until it was too late (Hanna, 2021).

Stuxnet is the most famous software described as an electronic weapon used in a cyberattack, and its design was intended to cause such damage. Therefore, it meets most definitions of a weapon, especially the intention of using it, but there is difficulty legally classifying it as a weapon. Regular legal weapons are not self-replicating and are unable to deploy independently or run automatic operations.

Figure 3 - On the Trail of the Stuxnet Worm (Goodin, 2014)

Zeus Trojan (Zbot) is a specific Trojan virus that targets Windows computers to extract sensitive financial information. A Zbot achieves this through man-in-the-browser (MitB) attacks, keystroke logging (keylogging), and form grabbing. Zbots are also able to launch CryptoLocker ransomware attacks (Certeza, 2013)**.** Zbot is a family of software that promises harmful viruses that disrupt the functionality of the entire computer system. The Zeus Trojan virus is designed to intercept interbank banking transactions. It spreads rapidly using phishing and may also spread by secretly hacking websites and creating security gaps in the user's browsing program (Lagrimas, 2022).

For example, when you hack into a computer on a bank site, the program recognizes and intercepts the bank's login information. It moves to it without alerting the user to a problem and then sends the information to a control server that may be located anywhere in the world. It can analyze the information obtained and come up with useful conclusions. The control server not only collects bank data but can also send updates, issue orders, and install additional software if the criminal chooses to do so (Unisys, 2010).

The software has been given the ability to receive updates to prevent detection by antivirus software and can also use stolen data to exploit the targeted system. If the infected system happens to be an industrial control system, the Zeus Trojan may be able to control or destroy the SCADA platform. This may adversely affect services or the entire state system.

Figure 4 - FBI Fraud Scheme Zeus Trojan (FBI, 2010)

Poison Ivy RAT is a remote access Trojan (RAT) that was first identified in 2005 and has continued to make headlines throughout the years. In 2011, it was used in the "Nitro" campaign that targeted government organizations, chemical manufacturers, human rights groups, and defense contractors (Cell, 2017). RAT is a remote access tool, which is a software application that allows users to interact

remotely as if they had physical access to a targeted computer system. It is like the Zeus Trojan but has broader applicability as a general-purpose remote access tool and is available free of charge online.

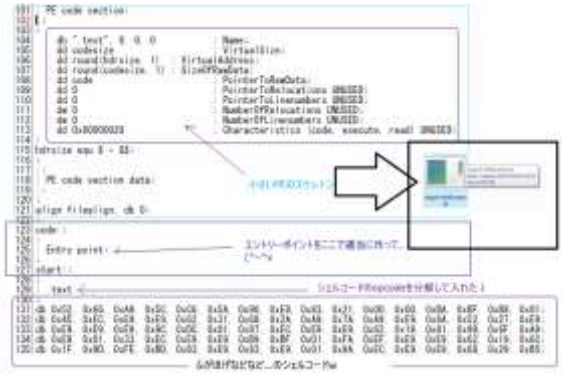

Figure 5 - Poison Ivy RAT (Paganini, 2017)

Low Orbit Ion Cannon (LOIC) is an open-source network stress testing and denial-of-service attack application written in C#. LOIC was initially developed by Praetox Technologies (Imperva, Low Orbit Ion Cannon (LOIC), 2020). However, it was later released into the public domain and is currently available on several open-source platforms. LOIC is free online software that allows any computer to participate in a very common attack called DDoS, or distributed denial of service. A DDoS attack is a cyberattack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users. This is done by temporarily or indefinitely disrupting the services of a host connected to a network. A denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests to overload systems. This is to prevent some or all legitimate requests from being fulfilled.

Attacking with this program is like having a group of people call a particular number at the same time. This exposes the phone line to excessive requests, not being able to handle all of them, and thus failing to connect. In this case, it is difficult to determine what can be considered a connected phone weapon. Therefore, it is very difficult to identify a factor that can be described as a weapon, whether it is a conventional weapon or an electronic one.

Figure 6 - Low Orbit Ion Cannon (Low Orbit Ion Cannon, 2021)

LOIC and Poison Ivy viruses can be considered computer-coded portable attack tools and can be examined to determine what they are and what they can do. This can be done by using the available information. It can be analyzed to see if it corresponds to the traditional concept of a weapon. This can be done to see how they can be dealt with and used under the law of war. However, cyberspace operations in which the primary factor is a smart human factor with an intuitive understanding of how the target system works are the most problematic. In these cases, it is very difficult to determine whether the worker should be the subject of a legal review to determine its legitimacy or not.

5. Cyberwarfare Weapons

War planning, both traditional and cyber, is subject to multiple legal reviews before proceeding, with legal advisers participating in the development of operations and arms reviews. This is to ensure that there is no negative impact on the civilian population, no unnecessary suffering of civilians or combatants, and compliance with the law of war.

As part of the evaluation of the legitimacy of the cyberattack operation, the

proposed capabilities and techniques that will achieve the desired impact on the target will be considered. As a result, military and electronic operations will be legitimate.

By understanding the complex nature of cybersecurity operations, it is critical to understand why it is imperative to solve cyber-weapon identification problems and the ability of armies to operate in cyberspace. Naming any capability as a weapon has legal and political implications. It cannot be used by armies until it is subject to legal review as part of the procurement process. This is because cyber capabilities are challenged by the difference between conventional weapons and electronic capabilities.

Much software is developed, and this gives "cyber weapon" a very broad meaning. There may not be enough jurists to review them all, and the program may become obsolete during the review process as the software is constantly updated. On the other hand, it may be difficult to formulate an objective test to determine when the capability, i.e., the previously reviewed weapon, needs a new legal review.

The Fourth Hague Convention Article 22, states: *"The right of belligerents to adopt means of injuring the enemy is not unlimited"* (ICRC, Annex to the Convention: Regulations respecting the laws and customs of war on land - Section II: Hostilities - Chapter I: Means of injuring the enemy, sieges, and bombardments - Regulations: Art. 22, 1907), and the regulations attached to it, stipulate that the right of combatants to adopt means of harming the enemy is limited, not absolute, as Article 36 of the First Additional Protocol of 1977 attached to the 1949 Geneva Conventions enshrined the requirement for legal reviews of all-new weapons, which states: *"An armistice suspends military operations by mutual agreement between the belligerent parties. If its duration is not defined, the belligerent parties may resume operations at any time, provided always that the enemy is warned within the time agreed upon, in accordance with the terms of the armistice"* (ICRC, Annex to the Convention: Regulations respecting the laws and customs of war on land - Section II: Hostilities - Chapter V: Armistices - Regulations: Art. 36., 1907)

As the purchase and use of weapons are subject to legal review, it is critical to choose the most appropriate definition of cyber weapons. An erroneous definition may lead to a failure to comply with international legal standards. In return, the very broad definition of the tools and techniques used in espionage can be covered and subjected to deep scrutiny. This would disrupt vital security operations in the state and make them vulnerable to bloody attacks (Nations, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 1977).

Because rules cannot be established that clearly answer all things that cannot be controlled in cyberspace, the focus is on answering the question: What is a cyber weapon? Any kind of war in the military sense means weapons capable of launching an attack. If the term "ground or air warfare" is to be expanded to include the concept of electronic warfare, then electronic weapons must be included alongside conventional weapons.

6. Cyber Armies

Defining electronic capability as a "weapon is a double-edged sword and a real problem" (Walker, 2020) because it sets an elusive standard in terms of the number of legal reviews, and cyber capabilities developed or acquired must be reviewed to ascertain their legitimacy under armed conflict law, domestic law, and international law before they are used in a conflict or military operation. This requires a

comprehensive legal review every time you change your computer program to function as a capability. Since this can happen dozens of times during an operation, the requirement is impractical. It is also an obstacle to the commander's ability to employ an effective military force in rapid cyberspace to achieve his or her operational objectives.

By contrast, electronic operations that do not constitute an attack are often conducted under international law without using anything that can be defined as a weapon. This would eliminate the need for a series of legal reviews. However, it would not eliminate operational legal review requirements that must match the capability used with the results of the planned process to ensure compliance with international law.

While there is no single specific definition of a weapon, the term is sufficiently popular in its use and in how it is treated under international law. A weapon "is designed for the primary purpose of killing, maiming, injuring, damaging, or destroying." This appropriate definition of conventional weapons can also be used as a definition of cyber weapons to ensure compliance with international law, particularly in the absence of clear guidance in Internet operations. It may make sense to harmonize definitions related to cyber operations with those used in conventional military operations (Pool, 2013).

The proposed definition provides a logical definition of a cyberattack, which can then be described as an electronic operation using an automated weapon. More specifically, a cyberattack can be defined as a process that uses technological means for killing, maiming, injury, or destruction (Vitkov, 2019), which would clarify when the laws of war apply to electronic operations and open a debate on issues surrounding cyber operations that fall short of the use of force, which make up the vast majority of cyber operations that are currently taking place. They are done without coherent rules of conduct and control (Weimann, 2004).

Although there are advantages to identifying a cyberweapon, there are also potential drawbacks to this definition. Strict identification of cyber weapons would eliminate the need for most legal reviews before operational planning. Although legal review remains required before any electronic technology is used in a process that addresses possible violations of international law, subsequent legal review wastes time and resources in the development of this technology, and this can be addressed through a conscious review of electronic warfare methods, a review of the legality of the distribution of harmful cyber capabilities, and the cessation of indiscriminate and uncontrolled distribution and illegality.

An in-depth analysis of the proposed definition of cyber weapons reveals the intriguing conclusion that the Internet is the only area of military operations in which the state can directly cause significant material harm to the adversary or enemy without the use of a weapon. The operational legal review will continue to address the concerns of international law. This is whether those concerns are the result of the means used, the method adopted, or the proportionality of use between means and purpose. It remains the intention and impact of the operation that will govern its legitimacy. Cyberspace is unique enough to justify this result to some extent.

Concluding remarks

Although the term "cyberweapon" became part of the general culture and circulated more than conventional weapons, there was no real consensus on its correct definition. The term was used to identify sets of computer codes that lead to different effects, from slowing websites

to destroying nuclear power plants, as in the Iranian case. This wide range of possibilities makes it difficult to control electronic processes to ensure compliance with international law and humanitarian standards.

There must be a basis for the legal analysis of military operations in cyberspace that are below the level of use of force and not regarded as espionage, as the current framework for cyber espionage under international law is not specified or compatible with non-identification. In addition to the confusion between non-espionage electronic operations and cyberattacks, this hinders the analysis of the compliance of military electronic operations with the law of war. The first step in this process should be to develop practical definitions of cyberattacks and cyberweapons.

Although the need for a clear definition is clear, some of the definitions proposed are impractical in the context of electronic processes. The definition of a cyber weapon must be logical and usable by internet operators and their legal advisers. Most of the logical definitions reviewed fall short of the goal of being of assistance to operators. This is because these definitions are either too vague or too broad. This may require legal reviews of everything the military uses as a cyber weapon, as well as reviews of its repeated versions of software, which is operationally impossible.

The definition of cyberweapons must be linked to the definition of conventional weapons so that it deals only with objects whose primary use is as weapons. This is to kill, destroy, or maim. This would allow the use of international standards and conform to the approach adopted in the Tallinn Guide. These definitions will meet the needs of military operators. They will provide them with clear guidance and continue to provide effective protection for civilians from electronic operations that may be illegal under international law.

Cyber-online espionage is an act of intelligence gathering conducted through digital technologies and tactics. It is a form of espionage that involves monitoring and collecting information from computers, networks, and other digital sources. It can be used to monitor online activity and communications, steal data, disrupt operations, and obtain access to sensitive information. It often involves the use of malware, which is malicious software designed to infiltrate systems, steal data, and gain access to networks. Hackers can use malware to gain access to computers, networks, and other devices and then use the data they find to access information or disrupt operations.

Cyber-online espionage can also involve the use of social engineering tactics, such as phishing emails or fake websites, to gain access to confidential information. It can also include monitoring a target’s online activity, such as their browsing habits and social media posts, to gain insight into their activities and interests. In some cases, the target’s activity can be tracked by using malware or by using computer networks to transmit information.

The Cyber Operations Act is a law that defines the legal framework for the use of cyber operations in the United States. This law is designed to protect the nation’s critical infrastructure and the security of its citizens. The Cyber Operations Act is a crucial step in ensuring that the US can defend itself against cyberattacks.

However, the Cyber Operations Act is not without its challenges. One of the biggest challenges is defining what constitutes a "cyberattack". Under the Cyber Operations Act, a cyber-attack is defined as any intentional or malicious use of computer networks, systems, and services to disrupt, deny, or degrade the availability, integrity, or confidentiality of a computer or information system. However, this definition is very general, and there is a lack of

consensus within the legal community about what activities should be classified as cyber-attack.

Another challenge under the Cyber Operations Act is the lack of clarity about what the US government is allowed to do in response to a cyberattack. The Act does not specify what the US can do in a defensive or offensive capacity, which has led to a lack of clarity about the government's role in cyber-defense. This lack of clarity has led to some confusion among the public about the US government's cyber policies and practices. The Cyber Operations Act is a necessary step in ensuring the safety and security of the US and its citizens. However, the Act is still in its preliminary stages, and there is a need for further clarification and guidance to ensure that the US can effectively respond to cyber-attacks.

The most dangerous cyberattacks are those that target critical infrastructure, such as electricity grids and water systems. These attacks can disrupt essential services, cause physical damage, and even lead to loss of life. Another harmful type of cyberattack is ransomware, which is a type of malicious software that encrypts data and then demands payment to unlock it. These attacks can cause financial losses and disrupt business operations. Phishing attacks, which are attempts to gain access to sensitive information by posing as a legitimate entity, are also dangerous. These attacks can be used to steal passwords, credit card numbers, and other confidential information.

Finally, distributed denial of service (DDoS) attacks, which involve overwhelming a system with traffic, can cause websites and other online services to become unavailable. This can have a severe impact on businesses, as it can prevent customers from accessing their websites or services. Overall, the most dangerous cyberattacks are those that target critical infrastructure, cause financial losses, or disrupt business operations. These attacks can have a severe impact on businesses, individuals, and even entire nations.

As a brief conclusion, Cybersecurity has become an increasingly significant issue in international law, as the threat of cyberattacks continues to grow. Cybersecurity is the practice of protecting networks, systems, and programs from digital attacks. These attacks can be used to gain unauthorized access to sensitive data and disrupt operations. Cybersecurity under international law is the practice of applying legal principles to the protection of information and communications technologies (ICTs).

The first international legal framework for cybersecurity was the Council of Europe's Convention on Cybercrime. This convention established the first set of principles and rules for international cooperation in the investigation of cybercrimes and the protection of ICTs. It also established the legal framework for the prosecution of cybercrimes and the protection of victims.

The European Union has also taken steps to address cybersecurity. The European Union Agency for Network and Information Security (ENISA) is responsible for developing and promoting the implementation of EU-wide cybersecurity policies. The agency has developed several initiatives and programs to promote the adoption of cybersecurity measures among EU member states.

At the global level, the United Nations has also taken steps to address cybersecurity. In 2015, the United Nations General Assembly adopted a resolution on the "Promotion, Facilitation, and Regulation of Information and Communications Technology (ICT)". This resolution calls for the establishment of a global cybersecurity system.

In addition to these international legal frameworks, individual countries have also taken steps to protect their citizens from cyberattacks. Many countries have adopted laws and

regulations that require organizations to implement cybersecurity measures. These measures can include the use of encryption, secure authentication, and access control.

Overall, international law plays an increasingly critical role in the protection of ICTs from cyberattacks. Cybersecurity is a global issue that requires global solutions. International legal frameworks, such as the Convention on Cybercrime and the European Union's ENISA, provide a foundation for countries to develop their laws and regulations to protect their citizens from cyberattacks.

Bibliography

Badawi, H. (2022). Tallinn Manual as a Legal Approach towards Cyber Warfare. *DIGITAL SOVEREIGNTY AND CYBERSECURITY* (pp. 69-74). МОСКВА: РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА . Retrieved from https://ui-miit.ru/files/docs/forum_tssik_sbornik_2022.pdf?fbclid=IwAR0242-lINsV2gDfMDqvODswRdR18BEaUz7BmHfwbFinVruKyJh4Hff-P30#%5B%7B%22num%22%3A72%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C41%2C535%2C0%5D

Bateman, J. (2022). *The Purposes of U.S. Government Public Cyber Attribution.* Washington: Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2022/03/28/purposes-of-u.s.-government-public-cyber-attribution-pub-86696

Cell, N. J. (2017). *Poison Ivy*. Retrieved from OFFICIAL SITE OF THE STATE OF NEW JERSEY: https://www.cyber.nj.gov/threat-center/threat-profiles/trojan-variants/poison-ivy

Certeza, R. (2013, October 31). *Ransomware Raises the Stakes With CryptoLocker*. Retrieved from Trend Micro: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3132/ransomware-raises-the-stakes-with-cryptolocker

Chen, T. (2014, June 1). CYBERTERRORISM AFTER STUXNET. *Strategic Studies Institute*. Retrieved from https://www.jstor.org/stable/resrep11324

Crime, U. N. (2022). *Offences against the confidentiality, integrity and availability of computer data and systems.* Retrieved from Katharina.kiener-manu: https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html

Crowther, G. (2017). The Cyber Domain. *The Cyber Defense Review*, pp. 63-78. Retrieved from http://www.jstor.org/stable/26267386

FBI. (2010). *Cyber Banking Fraud*. Retrieved from Federal Bureau of Investigation: https://archives.fbi.gov/archives/news/stories/2010/october/cyber-banking-fraud

Goodin, D. (2014). *Stuxnet worm infected high-profile targets before hitting Iran nukes*. Retrieved from Ars Orbital Transmission: https://arstechnica.com/information-technology/2014/11/stuxnet-worm-infected-high-profile-targets-before-hitting-iran-nukes/

Haig, Z. (2015). Electronic warfare in cyberspace. *Security and Defence Quarterly*, pp. 22–35. doi:10.5604/23008741.1189275

Hanna, A. (2021, November 1). *The Invisible U.S.-Iran Cyber War*. Retrieved from United States Institute of Peace: https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war

How Do SCADA Systems Work? (2022). Retrieved from Digital Prototype Systems Inc.: https://www.dpstele.com/scada/how-systems-work.php

I, P. (1977, June 8). *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts.* Retrieved from https://ihl-

databases.icrc.org/applic/ihl/ihl.nsf/ART/470-750056?OpenDocument

ICRC, d. (1907, October 18). *Annex to the Convention: Regulations respecting the laws and customs of war on land - Section II: Hostilities - Chapter I: Means of injuring the enemy, sieges, and bombardments - Regulations: Art. 22.* Retrieved from International Committee of the red cross: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/ART/195-200032?OpenDocument

ICRC, d. (1907, October 18). *Annex to the Convention: Regulations respecting the laws and customs of war on land - Section II: Hostilities - Chapter II: Spies - Regulations: Art. 29.* Retrieved from International Committee of the Red Cross: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=090BE405E194CECBC12563CD005167C8

ICRC, d. (1907, October 18). *Annex to the Convention: Regulations respecting the laws and customs of war on land - Section II: Hostilities - Chapter V: Armistices - Regulations: Art. 36.* Retrieved from International Committee of the red cross: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=7045DBD1E7D854B1C12563CD00516830

ICRC, d. (1907, October 18). *Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land.* Retrieved from International Committee of the Red Cross: https://ihl-databases.icrc.org/ihl/INTRO/195

ICRC, d. (1977). *Practice Relating to Rule 107. Spies.* Retrieved from International Committee of the Red Cross: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule107

Imperva. (2020, September 30). *Low Orbit Ion Cannon (LOIC)*. Retrieved from DDoS tools: https://www.imperva.com/learn/ddos/low-orbit-ion-cannon/

Imperva. (2022). *Advanced persistent threat* . Retrieved from APT: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

Justice, J. W., & Bricker, B. J. (2019, September 1). Hacked: Defining the 2016 Presidential Election in the Liberal Media. *Rhetoric and Public Affairs*, pp. 389–420. doi:10.14321/rhetpublaffa.22.3.0389

Lagrimas, D. (2022). *ZeuS and Its Continuing Drive Towards Stealing Online Data*. Retrieved from Trend Micro: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/64/zeus-and-its-continuing-drive-towards-stealing-online-data

Lee, M. R. (2017). APT(ADVANCED PERSISTENT THREAT)S AND INFLUENCE: CYBER WEAPONS AND THE CHANGING CALCULUS OF CONFLICT. *The Journal of East Asian Affairs*, pp. 39-64. Retrieved from APT: https://www.jstor.org/stable/44321272

Low Orbit Ion Cannon. (2021, July 17). Retrieved from SourceForge: https://a.fsdn.com/con/app/proj/loic/screenshots/220491.jpg/max/max/1

Merriam-Webster. (2022). *Definition of espionage*. Retrieved from Dictionary by Merriam-Webster: https://www.merriam-webster.com/dictionary/espionage

Nations, C. o. (1977, June 8). *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts.* Retrieved from United Nation - Office of Legal Affairs: https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and

Nations, C. o. (2016, August 23, 2016 23). *Chapter VII — Action with respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression.* Retrieved from United Nations -

Office of Legal Affairs: https://legal.un.org/repertory/art51.shtml

Nations, C. o. (2021, March 10). *Chapter I — Purposes and Principles.* Retrieved from United Nations - Office of Legal Affairs: https://legal.un.org/repertory/art2.shtml

Oona A. Hathaway, R. C. (2012, August). The Law of Cyber-Attack. *California Law Review*, pp. 817-885 . Retrieved from https://www.jstor.org/stable/23249823

Paganini, P. (2017, March 17). *New APT Campaign based on Poison Ivy RAT with C&C*. Retrieved from Security Affairs: https://securityaffairs.co/wordpress/57212/apt/poison-ivy-rat-china.html

Pool, P. (2013). War of the Cyber World: The Law of Cyber Warfare. *The International Lawyer*, pp. 299-323. Retrieved from https://www.jstor.org/stable/43923953

Prochko, V. (2018, March 30). *The International Legal View of Espionage.* Retrieved from E-International: https://www.e-ir.info/2018/03/30/the-international-legal-view-of-espionage/

Sampalli, D. U. (2020, February). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*. doi:10.1016/j.cose.2019.101666

Unisys. (2010). *Zeus Malware: Threat Banking Industry.* Unisys Corporation. Retrieved from https://botnetlegalnotice.com/citadel/files/Guerrino_Decl_Ex1.pdf

Vitkov, E. E. (2019, June). *Cyberwarfare and Collateral Damages*. Retrieved from Hauser Global Law School Program: https://www.nyulawglobal.org/globalex/Cyberwarfare_Collateral_Damage1.html

Walker, J. (2020). The Double-Edged Sword Of Digital Transformation. *Forbes Technology Council*, https://www.forbes.com/sites/forbestechcouncil/2020/08/04/the-double-edged-sword-of-digital-transformation/?sh=74e9ab621d0a .

Weimann, G. (2004). *Cyberterrorism, How Real Is the Threat?* Washington: UNITED STATES INSTITUTE OF PEACE. Retrieved from https://www.usip.org/sites/default/files/sr119.pdf