Forum: GA3-Legal

Issue: Regulating cyber warfare frameworks under International Law

Student Officer: Nazlı Emre

Position: President Chair

Introduction

Technology has become a huge part of all of our lives and nations are growing increasingly reliant on digital infrastructure to manage essential services such as healthcare, banking, national security, etc. The downside of using technology in governing is the potential of cyberattacks and the disruption and damage these attacks can cause. Unlike traditional armed war, cyber wars take place in the shadows. Cyber warfare is the use of digital attacks by state or non-state actors to achieve military or political objectives. Stealing sensitive data, disabling critical infrastructure, manipulating public information, interfering with a democratic process and many more can be categorized as cyber warfare. Since these acts are committed on a digital platform and not physically, they are hard to detect and nearly impossible to predict. A cyberattack can originate from one country, be routed through multiple other countries, or be carried out by a non-state proxy. The endless possibilities make accountability and retaliation complicated.

International law, UN charters, conventions, treaties, frameworks, etc. provide legal rules and standards for physical warfare. However, there is little to no legal guidance on how to regulate or punish digital warfare. The lack of international treaties on cyber warfare has resulted in legal and ethical gray areas. This situation raises a lot of questions. Is it possible to prove who committed a cyberattack? Is it ethically right to accuse or punish someone or a country for committing a cyberattack if there is no binding international treaty on cyber warfare? Do digital breaches also count as a violation of a country's borders? Is spying or hacking into another country's data an act of war? These are some of the pressing questions that the world is facing today. The absence of binding legal standards endangers

international peace and security. It also creates a risk of civilian harm. Thus, addressing this issue is crucial in this evolving world.

Definition of Key Terms

Cyber warfare

Cyber warfare is "the strategic deployment of cyber attacks by a nation-state or international organization to target another country's national security, civil infrastructure, or civic infrastructure" (American Public University). Cyberattacks usually target the essential infrastructure of countries. Cyber espionage, ransomware attacks, hacking, malware, denial-of-service attacks, etc. are kinds of cyber warfare.

Cyber operations

Cyber operations is a broader term for cyber warfare. These include all actions taken in cyberspace to achieve military, intelligence, economic or political objectives. These operations do not necessarily reach "war" level.

Attribution

Attribution is the process of identifying who is responsible for a cyberattack. This is particularly hard because of anonymity, use of proxies, technical obfuscation, etc.

International humanitarian law (IHL)

International humanitarian law, also known as the law of armed conflict, "is a set of rules which seek, for humanitarian reasons, to limit the effects of armed conflict. It protects persons who are not or are no longer participating in the hostilities and restricts the means and methods of warfare" (The International Committee of the Red Cross).

Proportionality

"Proportionality in human rights law means identifying the various options available and choosing the one which is least restrictive of a person's human rights to achieve the legitimate aim" (The British Institute of Human Rights). Proportionality

requires that any military action including cyberattacks to avoid excessive harm to civilians.

Cyber deterrence

Cyber deterrence is a strategy used to deter cyber attacks from occurring. This discouragement is created through fear of consequences.

Non-state actors

Non-state actors are individuals or groups such as hacktivists or cybercriminals who work independently out of government control. Most of these are supported or sponsored by governments.

Critical infrastructure

Critical infrastructure is the term used for systems and assets essential for a country to function properly. These are usually targeted in cyberattacks.

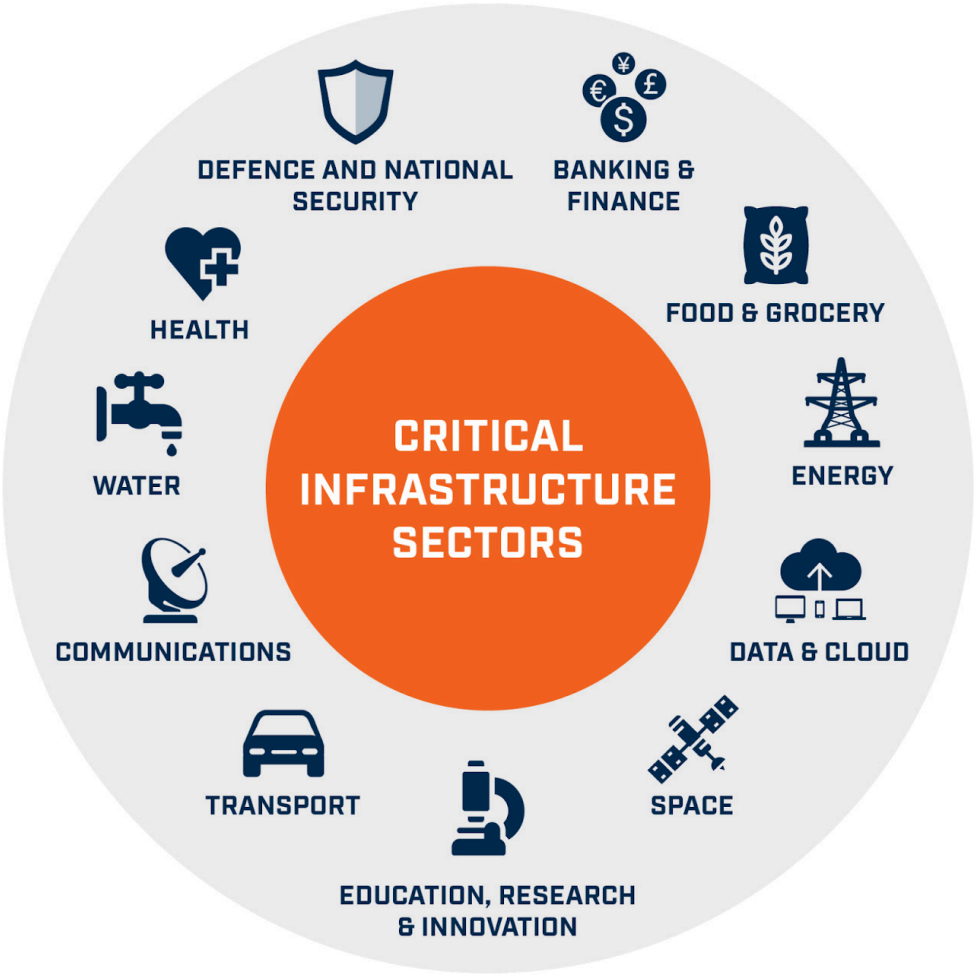

Image 1: Critical infrastructure sectors

Denial-of-service (DoS) attack

Denial-of-service attacks aim to shut down a system or network by overwhelming it with traffic. These attacks flood a system, website or network with excessive requests and this causes it to slow down or crash and become unavailable to users.

Malfare

"Derived from 'malicious software', malware is any kind of software that can damage computer systems, networks or devices. Includes viruses, ransomware and trojans" (National Cyber Security Center).

Background Information

Cyber warfare takes place in cyberspace which defies the usual battlefields of war. It does not involve direct physical force or harm. This doesn't mean that cyber warfare doesn't do any damage. Instead of weapons, it does damage through malicious software, unauthorized access or network manipulation. Cyber attacks can shut down national power grids, paralyze government systems or military communication, interrupt emergency services, corrupt financial systems, leak or steal sensitive data, manipulate public opinion or elections through misinformation, etc. The problem is, these attacks are usually sudden and unpredictable. So, the damage is already done once it gets noticed. There are many objectives of cyber warfare. Espionage and sabotage are the most common ones. Deterrence or coercion are also strong motives.

The Challenges of Cyber Warfare

There are many aspects that make this a complicated issue. Attribution is one of them. After a cyber attack, the first step is to determine who is responsible. This is difficult do to many reasons. Cyber attacks can be routed through multiple servers all around the world. The attackers usually use encryption, proxy networks, false flag tactics, etc. to disguise their identities. Non-state actors also act independently or on behalf of a country. Without being able to identify who is responsible, it is hard to

take legal action towards punishment. Accusing the wrong party would cause unnecessary conflict between countries and they tried to avoid this. Assuming they managed to correctly find the responsible party, there is still legal ambiguity and a lack of regulation. The existing international law is unclear when it comes to cyber warfare. There is no universally accepted definition of cyber warfare. More importantly, there is no clear definition of "use of force". The International Humanitarian Law was designed for physical warfare and it does not apply to digital scenarios. There is a debate over whether cyber operations during peacetime can be considered acts of aggression under the UN charter. This legal aspect of the issue will be further discussed in the legal grey zone part down below.

Jurisdiction and sovereignty also create challenges. Cyberattacks often cross borders and affect systems located in multiple countries. Cyber operations can pass through multiple jurisdictions. They can go through dozens of countries' networks, thus crossing digital borders. This situation raises questions about whether a country can take countermeasures if the attack originated from another country. Many countries disagree on whether these cyber activities violate sovereignty. This makes international cooperation and enforcement difficult since some countries refuse to acknowledge responsibility or lack the capacity to control digital activity inside their borders. If there is a misunderstanding between countries about the intention or origin of a cyber attack, it could lead to further conflict. These attacks are often invisible or silent. So, countries might not realize it happening until systems fail. Some countries might interpret these attacks as an act of war. Wrong attribution increases the risk of further conflict. The concern here is how easily one of these misunderstandings can escalate into physical conflict. Physical conflict should be avoided at all costs in order to prevent civilian damage. Additionally, cyber attacks usually target or impact civilian infrastructure. Many cyber attacks disable hospital systems or public transportation networks, interrupt water or energy supplies, spread disinformation to destabilize societies, etc. During conventional war, civilians are protected under the law. The International Humanitarian Law legally prioritizes

civilians. In cyber warfare, laws do not protect civilians. Unlike traditional war, civilians are on the front lines of war in cyber warfare. This is the main concern.

Additionally, there is a lack of shared norms and trust between countries. There is no global consensus on what behavior in cyberspace is acceptable or unacceptable. Some countries support a free and open internet while others prefer state control over cyberspace. The differences of opinion and lack of trust between major cyber powers make international cooperation unachievable. Without universally accepted and agreed-upon norms, it is difficult to set boundaries or prevent malicious cyber behavior. It is also important to acknowledge that technology keeps rapidly changing. Technology evolves faster than international law. New vulnerabilities such as IA are emerging every day. Governments and institutions struggle to keep up with both defensive and offensive developments. Regulation efforts are constantly trying to keep up with technology and these difficulties make it harder.

The Legal Grey Zone

There is an absence of universally accepted legal definitions of terms like cyber warfare, use of force or armed attack. This leads to uncertainty over when a cyber attack becomes legally equivalent to an act of war or whether a state has the right to respond with force. What constitutes “use of force”? Or is it just an act of sabotage? According to Article 51 of the UN Charter, “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”. This article states that countries have the right to self-defense against

an armed attack. But what counts as an armed attack? This grey zone is what makes this issue dangerous. The uncertainty is open to different interpretations.

"The term cyber warfare refers to means and methods of warfare that rely on information technology and are used in situations of armed conflict. Cyber operations may be either offensive or defensive. IHL only applies to cyber operations that occur during – or that themselves trigger – an armed conflict" (The International Committee of the Red Cross). Isn't disrupting a hospital's electric supply the same as physically bombing it? This is where it gets complicated. The existing international law is not enough. The nature of cyber conflict is so different that it needs entirely new laws or treaties. Another option is interpreting the already existing law for the cyber domain. Until now, efforts to create a binding international treaty specifically for cyber warfare have not succeeded because of political disagreements, trust issues and competing national interests. There is an urgent need for regulation because the absence of legal clarity increases the risk of misinterpretation, escalation and harm to essential systems or civilians. Until there is a universally accepted framework, cyberspace will remain a lawfully uncertain and dangerous place.

Major Countries and Organizations Involved

The United States of America

The United States is one of the leading cyber powers in the world. It has one of the most advanced cyber warfare infrastructures. The U.S. Cyber Command (USCYBERCOM) was established in 2010 and it deals with these infrastructures. It has a strong military strategy and both defensive and offensive capabilities. The U.S. has been involved in many cyber operations, the most known one being the Stuxnet attack on Iran's nuclear program. This attack is considered the first cyber weapon to cause physical destruction. The U.S. argues that the already existing international law also applies to behavior in cyberspace. It supports the Tallinn Manuals. It plays an important role in UN forums like the GGE and OEWG. It has also pushed back against proposals for a new binding treaty that emphasizes state sovereignty over

cyberspace by countries like Russia and China. This means that the U.S. sees cyberspace as a potential tool for authoritarian control. Still, the U.S. promotes international cooperation on cyber defense through NATO and bilateral and multilateral agreements. It has also significantly invested in cyber threat intelligence, attribution and deterrence. The Cybersecurity and Infrastructure Security Agency (CISA) plays an important role in the country's cyber defense. The U.S. also supports the UN's 11 voluntary norms.

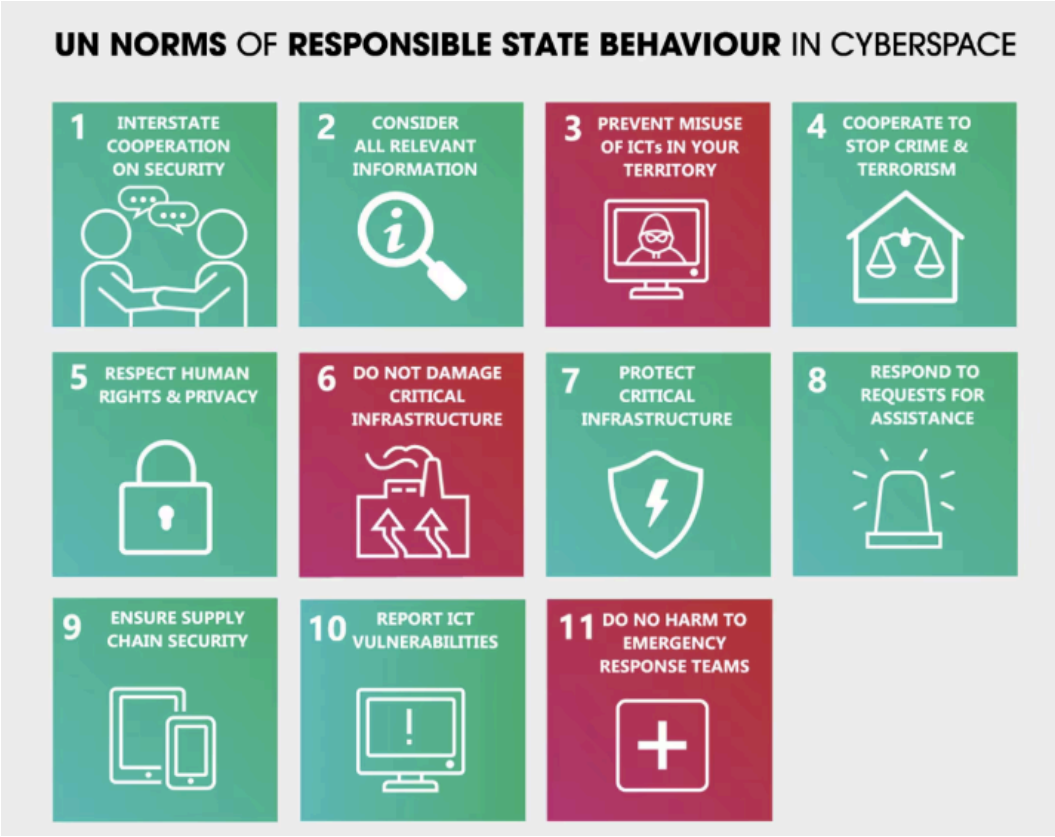

Image 2: UN norms of responsible state behaviour in cyberspace

Russia

Russia is one of the top cyber powers in the world and has advanced offensive cyber capabilities. It is frequently accused of launching state-sponsored cyber operations against both military and civilian targets worldwide. Russia has been linked to many high-profile cyber incidents such as the 2007 Estonia cyberattacks, 2015 and 2016 Ukraine power grid attacks, interference in the 2016 U.S. presidential elections, the 2017 NotPetya malware attack and many more. Russia has

a completely different opinion from the U.S. and its allies. It does not accept that the aşready existing law is enough and supports the creation of a new law. Russia is also involved with the GGE and OEWG.

China

China is a major global cyber power because of its technological capacity and strategic influence. It has extensive cyber warfare capabilities. The People's Liberation Army (PLA) Strategic Support Force handles cyber warfare. China is frequently linked to cyber espionage and intellectual property theft. China argues that the already existing international law is not enough to regulate cyberspace and cyber warfare and wants to create a new international treaty. China is involved with the GGE and OEWG. China is against the Budapest Convention on Cybercrime. It argues that it was developed without universal participation and might threaten national sovereignty. China proposed the Global Initiative on Data Security in 2020.

Iran

Iran developed its cyber capabilities after the Stuxnet attack in 2010. This joint U.S.-Israeli cyber operation damaged its nuclear centrifuges. Iran has been linked to many cyber operations mainly targeting USA, Israeli, Saudi and Gulf interests. There was the Shamoon attack in 2012 and the DDoS attacks between 2011 and 2013. Iran argues that the already existing international law should also apply to cyberspace. Iran is not a part of the Budapest Convention on Cybercrime. Iran works with the OEWG. Iran has been a victim of cyber aggression multiple times from the U.S. and Israel. Even though Iran is not a major power like the U.S., China or Russia, it is a rising power.

North Korea

Since the early 2000s, North Korea has invested in cyber capabilities. Due to its extensive capabilities, it has been linked to many high-profile cyber operations such as the 2014 Sony Pictures Hack, the SWIFT Banking attacks between 2015 and 2018, the 2017 WannaCry ransomware attack and many more. North Korea has not stated an opinion on the legal aspect of this issue. It works independently.

The European Union

The EU plays a leading role in the creation of a new international law and multilateral cooperation. It prioritizes human rights in cyberspace. It aims for a secure, stable and open cyberspace. The European Union strongly supports that the already existing international law should be adapted to cyberspace. The EU is involved with the GGE and OEWG. The EU has implemented a cyber sanctions regime which imposes restrictive measures on individuals and entities responsible for major cyber attacks. It also promotes international cooperation and diplomacy.

India

India invested in cyber infrastructure and cybersecurity by establishing multiple national institutions. It has faced many cyber threats mainly from China and Pakistan. There have been multiple attacks on its critical infrastructure. India supports the adaptation of the already existing international law to cyberspace. India did not sign the Budapest Convention on Cybercrime because of its concerns about national sovereignty and the lack of UN involvement during its drafting. India is involved with the OEWG.

The United Nations

The United Nations supports that the already existing international law also applies to cyberspace. These are the 1945 UN Charter, The International Humanitarian Law (IHL) and The International Human Rights Law (IHRL). The UN's Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG) are working towards the issue. The GGE has published several reports. There are also many UN resolutions on the issue. These could be found in the Relevant UN Resolutions and Other Documents section. The UN Office for Disarmament Affairs (UNODA) also supports the GGE and OEWG.

The International Committee of the Red Cross (ICRC)

The International Committee of the Red Cross promotes the application of the International Humanitarian Law (IHL) to cyber warfare. The ICRC does not engage in political or military matters. It's one and only concern is protecting civilians. The ICRC argues that the already existing IHL applies to cyber operations conducted during

armed conflict. It has published many reports and legal analyses on the implications of cyber warfare. The ICRC is a neutral organization without a side. It only supports humanitarian matters.

The North Atlantic Treaty Organization (NATO)

NATO has an important role in global cybersecurity. In 2016, NATO declared that cyberspace is a domain of operations. This means that cyberattacks can be addressed as military threats. NATO argues that the already existing international law also applies to cyberspace. NATO supports the GGE and OEWG. It also cooperates with the European Union.

Timeline of Events

Date	Description of event
2 November 1988	The Morris worm is released. First ever internet attack.
1990s	Militaries start using technology. First cyber espionage and sabotage incidents.
23 November 2001	The Budapest Convention on Cybercrime is signed.
2007	Estonia cyber attacks take place. First major politically motivated cyber attack.
2010	Stuxnet worm incident. A joint U.S.-Israeli cyber operation targeting Iran's nuclear facilities. First known cyber weapon to cause physical destruction.
24 June 2013	The first UN Group of Governmental Experts (GGE) report is released.
2013	Tallinn Manual 1.0 is published.

2015	The UN GGE agrees on 11 voluntary norms of responsible state behaviour in cyberspace during peacetime.
16 October 2015	U.S.-China Cyber Crime Agreement is signed.
2017	Tallinn Manual 2.0 is published.
2017	WannaCry (North Korea) and NotPetya (Russia) attacks. Two global ransomware and malware campaigns cost billions in damage.
12 March 2021	The United Nations Open-Ended Working Group (OEWG) published its first report.
2022	Russia-Ukraine cyber attacks occur during the war.

Relevant UN Resolutions and Other Documents

- Resolution adopted by the General Assembly on 24 December 2024, Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (A/RES/79/243)
- Resolution adopted by the General Assembly on 23 December 2015, Developments in the field of information and telecommunications in the context of international security, (A/RES/70/237)
- Resolution adopted by the General Assembly on 5 December 2018, Developments in the field of information and telecommunications in the context of international security, (A/RES/73/27)
- Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 14 July 2021, (A/76/135)

- Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, (A/70/174)
- Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013, (A/68/98)
- Open-ended working group on security of and in the use of information and communications technologies 2021–2025 established pursuant to General Assembly resolution 75/240, 8 October 2024, (A/C.1/79/L.13)
- Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report, 10 March 2021. (A/AC.290/2021/CRP.2)
- The U.S.–China Cyber Agreement, 16 October 2015, https://sgp.fas.org/crs/row/IN10376.pdf
- JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013, https://www.eucybernet.eu/wp-content/uploads/2020/08/2013-cybersecurity-strategy-of-the-european-union.pdf
- NATO Cyber Defence Pledge, 8 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm
- The North Atlantic Treaty, 4 April 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm
- United Nations Charter, https://www.un.org/en/about-us/un-charter/full-text
- The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols, Council of Europe, https://www.coe.int/en/web/cybercrime/the-budapest-convention
- United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of

Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

- 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law, https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/
- The UN norms of responsible state behaviour in cyberspace, Guidance on implementation for Member States of ASEAN, International Cyber Policy Center, March 2022, https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

Previous Attempts to Solve the Issue

- UN efforts: The Group of Governmental Experts (GGE) released reports in 2010, 2013, 2015 and 2021. They proposed the 11 norms of responsible state behaviour. But, these didn't turn out to be so effective since they are non-binding. Also, some of the GGEs didn't agree because of political divisions specifically between Western countries and authoritarian states. The Open-Ended Working Group (OEWG) is more inclusive than the GGE and includes more UN member states. They tried to promote transparency and cooperation. They released a report in 2021.
- The Tallinn Manuals: The Tallinn Manual 1.0 was published in 2013 and the Tallinn Manual 2.0 was published in 2017. These were developed by the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE). The importance of these documents are how academic they are. They include legal analyses of how the already existing international law applies to cyber operations. Still, they are non-binding. They are not officially endorsed by state governments and their authority is interpretative instead of legislative.

- NATO: In 2014, NATO declared that a cyberattack could trigger Article 5. “Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security” (NATO). This means that it could justify collective defense. NATO also adopted the Cyber Defence Pledge in 2016.
- Frameworks: The European Union adopted a Cybersecurity Strategy in 2013. This was revised and updated in 2020. The U.S.-China Cyber Agreement was signed in 2015. Also, there was the Budapest Convention on Cybercrime in 2001.

Possible Solutions

There are two main ways to go with this issue. The first one is developing a new binding international treaty on cyber warfare. Establishing a globally agreed and legally binding framework is an option. This framework should include clear definitions of cyber attack, cyber warfare and cyber weapon. It should include rules prohibiting attacks on critical civilian infrastructure. A framework like this would have legal clarity, universal application and stronger enforcement. But, it would be hard to negotiate because of conflicting interests and geopolitical tensions. The second option is to interpret the already existing international humanitarian law to apply to cyberspace.

Other than these two, there are many other things we can do. Establishing an independent attribution and investigation body is a good idea. This would be a neutral and international organization which would investigate and attribute cyber attacks. An organization like this would reduce false accusations and support accountability. Another idea can be adopting confidence-building measures (CBMs) between states. These would be practical and could be helpful to avoid escalation. It would also increase predictability. But, since these would be voluntary they can't be enforced.

Additionally, we can encourage countries to adopt and update cybercrime and cyber warfare laws that are aligned with international norms. These could be supported through capacity-building and legal harmonization. Capacity-building would help less developed countries to improve cyber resilience, legal frameworks and attribution capabilities. And legal harmonization would make consensus easier and reduce disagreements.

Bibliography

CCDCOE.

ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law.

"Critical Infrastructure Protection." *Drishti IAS*,

www.drishtiias.com/daily-news-editorials/critical-infrastructure-protection.

"Cyber Conflict in the Russia-Ukraine War." *Carnegie Endowment for International Peace*,

carnegieendowment.org/programs/technology-and-international-affairs/cyber-conflict-in-the-russia-ukraine-war?lang=en.

Nato. "Cyber Defence Pledge." *NATO*,

www.nato.int/cps/en/natohq/official_texts_133177.htm.

Melzer, Nils. "Cyberwarfare and International Law." *UNIDIR RESOURCES*, 2001,

unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf.

Eleven Norms of Responsible State Behaviour in Cyberspace.

www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2021/04/uno-cyber-normen.html.

Home | How Does Law Protect in War? - Online Casebook. casebook.icrc.org.

"Malware." *National Cyber Security Center*, www.ncsc.gov.uk/section/advice-guidance/all-topics?topics=Malware&sort=date%2Bdesc.

"The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols." *Council of Europe*, www.coe.int/en/web/cybercrime/the-budapest-convention.

"The Morris Worm." *FBI News*, 2 Nov. 2018, www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

Nato. "The North Atlantic Treaty." *NATO*, www.nato.int/cps/en/natohq/official_texts_17120.htm.

Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum*, 24 May 2024, spectrum.ieee.org/the-real-story-of-stuxnet.

The Tallinn Manual. ccdcoe.org/research/tallinn-manual.

Hogeveen, Bart. "The UN norms of responsible state behaviour in cyberspace." *International Cyber Policy Center*, Mar. 2022, documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.

"UN Cybercrime Convention - Full Text." *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html.

United Nations. "United Nations Charter (Full Text) | United Nations." *United Nations*, www.un.org/en/about-us/un-charter/full-text.

Hern, Alex. "WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017." *The Guardian*, 30 Dec. 2017, www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.

Slonopas, Andre. "What Is Cyber Warfare? Various Strategies for Preventing It." *American Public University*, 3 May 2024, www.apu.apus.edu/area-of-study/information-technology/resources/what-is-cyber-warfare.

The International Committee of the Red Cross. "What is International Humanitarian Law?" *ADVISORY SERVICE ON INTERNATIONAL HUMANITARIAN LAW*, July 2004, www.icrc.org/sites/default/files/external/doc/en/assets/files/other/what_is_ihl.pdf.

"What Is Proportionality? | British Institute of Human Rights." *British Institute of Human Rights*, www.bihr.org.uk/get-informed/legislation-explainers/what-is-proportionality#:~:text=Proportionality%20in%20human%20rights%20law,to%20achieve%20the%20legitimate%20aim.