Forum:	Security Council (SC)
Issue:	Casus Belli and the Right to Self-defense in Cyberspace
Student Officer:	Christos Liosis
Position:	Deputy President

PERSONAL INTRODUCTION

Dear delegates,

First and foremost, I am honored to address you all as a part of this year's PS Model United Nations conference. My name is Christos Liosis, and I am thrilled to be serving as one of your chairs for this year's conference. This is my second time chairing, and my experiences include five conferences in Greece and two in the United States of America. Throughout my MUN journey and engagement in global affairs, I have developed a keen interest in diplomacy and international relations.

In this study guide, you will be provided with important information regarding the second topic on this year's Security Council agenda, namely "Casus Belli and the Right to Self-Defense in Cyberspace". The guide will delve into the multifaceted dimensions of Casus Belli and the Right to Self-defense in Cyberspace, examining historical precedents, which nations have been involved and some previous attempts to solve this problem. It is my fervent hope that this guide will serve as a reliable resource and give you inspiration to produce your own innovative resolutions. I strongly advise you to conduct further research on the subject since new information is being revealed every day.

Should you have any questions or require further clarification concerning either the topic, the mandate of the committee, or any other concerns, please feel free to contact me at christos.liosis@gmail.com

I am more than willing to support you in any way I can. I eagerly await the opportunity to meet each one of you.

Best regards,

Christos

INTRODUCTION

In the rapidly evolving landscape of international relations, the digital realm has emerged as a critical arena for global interactions. The limitless potential of cyberspace has not only facilitated unprecedented advancements but has also given

rise to new challenges and complexities. Among these challenges lies the pressing issue of an approximate threat of war due to cyberattacks. The international community still struggles to establish standards and guidelines for cyberspace, an ever-changing and constantly evolving domain. Governments and international organizations, which bear the primary responsibility for addressing this issue, are making great efforts to develop frameworks and agreements that will more effectively and legally bind them to address cyber threats, cyber espionage, and cyber warfare.

The idea of Casus Belli, or "cause of war," has become more important in the fast-developing world of cyberspace as a result of the rise in cyberattacks and their propensity to turn into military confrontations. In cyberspace, the term "Casus Belli" refers to major and harmful cyber operations that might be used as justification for a country to exercise its right to self-defense. International law defines self-defense as a state's right to use force in response to armed attacks and constitutes the only exception to the prohibition of the use of force. However, figuring out what qualifies as an armed attack and, therefore, as Casus Belli in cyberspace is still up for debate.

Setting a clear definition for what constitutes Casus Belli in the digital sphere is fraught with significant obstacles. The main challenge lies in the ambiguity surrounding when a cyberattack qualifies as an armed attack, triggering the right to self-defense. Due to the intangible and often stealthy nature of cyber operations, it can be difficult to determine the true origin, intent, and severity of a cyber incident. Accurately identifying the perpetrators of cyberattacks can be challenging because they can conceal their identities and take advantage of third-party infrastructure. In addition, unlike traditional armed attacks, it is difficult to accurately quantify the scale and damage caused by cyberattacks. This lack of clarity hinders the establishment of clear thresholds and criteria for justifying a military response in cyberspace, leading to uncertainty among states on when they can legitimately exercise the right to self-defense.

Therefore, the international community is faced with the following question: when does a cyberattack qualify as an armed attack, and by extension, when does the right to self-defense apply? The ability to defend oneself against an armed strike in cyberspace allows countries to deploy the required force, even if the attack starts in the online world. This raises another question concerning defining the proportionality of the response when dealing with a cyberattack. More specifically, in the event that a cyberattack does qualify as an armed attack, what are the appropriate means of self-defense that a state can exercise, and can they expand beyond the digital world into the world of traditional armed conflict? The international community needs to answer these questions and is faced with the challenge of striking a delicate balance between safeguarding national security and addressing cyber threats.

As we gather here under the conference theme of "Paradox of Progress," it is essential to recognize that cyberspace has provided avenues for connectivity and peacebuilding. The question of when cyber incidents amount to a justifiable cause for military action, and how the right to self-defense applies in such situations, requires great international cooperation.

The internet and interconnected systems have facilitated significant advancements in education, communication, and economic growth, fostering a sense of global unity. In the pursuit of progress, it is crucial to establish robust mechanisms for attribution and accountability in cyberspace. Delegates, you must all consider the implications of cyber incidents within the framework of international law, ensuring that your responses prioritize peace and stability while safeguarding the rights and sovereignty of nations.

In this study guide, we will delve into the multifaceted dimensions of Casus Belli and the Right to Self-defense in Cyberspace, examining historical precedents, which nations have been involved and some previous attempts to solve this problem.

DEFINITION OF KEY TERMS

Cyberspace

Cyberspace, the virtual realm where communication over computer networks takes place, plays a pivotal role in the Paradox of Progress. While it enables unprecedented connectivity and information sharing, it also facilitates cyberattacks, highlighting the inherent contradiction between technological advancement and security in our increasingly interconnected world.[1]

Casus Belli

A "Casus Belli" takes on new meaning in the arena of online. It denotes an act or scenario that acts as a provocation or excuse for hostile digital actions. As governments rely more and more on cyberspace for key infrastructure and communication, each large cyber incident can be viewed as a potential Casus Belli, highlighting the changing nature of conflict and warfare in the modern world.[2]

Right Of Self-Defense

Self-defense in international law refers to the inherent right of a State to use of force in response to an armed attack. Self-defense is one of the exceptions to the prohibition against use of force under article 2 of the UN Charter and customary

[1] 'The of the English Defines "cyberspace" as the Notional Environment in Which Communication over Computer Network Occurs.BE's New DictionaryOxford DictionaryUrban DictionarySamuel Johnson's Dictionary'. *Toppr Ask*, https://www.toppr.com/ask/question/the-of-the-english-defines-cyberspace-as-the-notional-environment-in-which-communication-over/.

[2] *CASUS BELLI | Η ΚΑΘΗΜΕΡΙΝΗ*. https://www.kathimerini.gr/tag/casus-belli/.

international law. The problem with the right to self-defense in cyberspace is that it is unclear under international law when a cyberattack constitutes an armed attack, and hence when nations can invoke the right to self-defense in cyberspace. As a result, the right to self-defense in cyberspace remains uncertain.[3]

Perpetrators

Individuals that conduct cybercrimes or engage in damaging actions in cyberspace are modern-day "perpetrators" or "offenders" in the context of the Paradox of Progress. This demonstrates how technology advancement has not only created new channels for communication and business, but has also given rise to a new breed of criminals who use the digital sphere for unlawful purposes. [4]

Espionage

Espionage is the covert and clandestine activity of gathering and uncovering sensitive information, particularly political or military secrets of a foreign country or the proprietary and industrial data of a nation. It involves the use of intelligence gathering techniques, such as surveillance, infiltration, codebreaking, electronic eavesdropping, and human intelligence operations, to access classified or confidential data without the knowledge or consent of the target country or organization.[5]

Sovereignty Of Nations

The principle of the Sovereignty of Nations is closely tied to Chapter 2.1 of the United Nations Charter, which emphasizes the respect for the sovereignty and territorial integrity of all member states. This chapter underscores the fundamental importance of each nation's autonomy and exclusive authority over its internal affairs and territories. It also sets the tone for peaceful cooperation among member states while upholding the principle of non-interference in the domestic affairs of other countries. Thus, the concept of sovereignty, as outlined in the UN Charter, serves as a cornerstone of international relations, promoting peaceful coexistence and cooperation among sovereign states.[6]

UN Charter

The Charter of the United Nations is the founding document of the United Nations. It was signed on June 26th, 1945, in San Francisco, at the conclusion of the United Nations Conference on International Organization and came into force on 24 October 1945.[7]

---

[3] *Self-Defence | How Does Law Protect in War? - Online Casebook*. https://casebook.icrc.org/a_to_z/glossary/self-defence.
[4] *Perpetrator*. 31 Jan. 2024, https://dictionary.cambridge.org/dictionary/english/perpetrator.
[5] *Espionage*. 31 Jan. 2024, https://dictionary.cambridge.org/dictionary/english/espionage.
[6] Sovereignty|MilwaukeePublicMuseum. https://www.mpm.edu/educators/wirp/nations/sovereignty
[7] Nations, United. 'UN Charter'. *United Nations*, https://www.un.org/en/about-us/un-charter.

Article 51 UN Charter

The United Nations Charter recognizes a nation's inherent right to self-defense in the face of an armed attack on one of its members. This principle reinforces a nation's sovereignty, highlighting its authority over internal matters and territory. However, it also highlights the balance between sovereignty and international cooperation. While nations maintain the right to defend themselves, the Charter emphasizes that self-defense should be a last resort, involving the Security Council to address threats to global peace. This dynamic showcases the complex relationship between sovereignty and the collective responsibility for global security and peace in international diplomacy, essential for both experienced diplomats and newcomers to the field of international relations.[8]

Vigilance Actions

The practice of maintaining careful attention, often referred to as vigilance, holds significant relevance within the context of the Sovereignty of Nations. Just as vigilance requires staying alert to potential dangers, nations must also remain watchful of any potential threats to their sovereignty. Sovereignty underscores a nation's independent authority over its internal affairs and territory, making it imperative for nations to exercise vigilance in protecting this autonomy. Vigilance in international relations ensures that nations remain aware of, and can respond to any actions or policies from other nations that might encroach upon their sovereignty. It stands as a crucial aspect of maintaining the delicate equilibrium between asserting national autonomy and engaging in cooperative diplomacy on the global stage.[9]

Non-State Actors

Non-state actors, such as cybercriminal groups, hacktivists, and state-backed proxies, play a crucial role in shaping how Casus Belli is defined in the realm of cyber conflict. When these non-state entities launch significant cyberattacks, potentially causing harm or posing national security threats, they can trigger considerations of self-defense or retaliatory actions by states. However, the challenge lies in accurately attributing these attacks, as non-state actors often operate covertly and from various locations. This complexity adds intricacy to determining what qualifies as a justifiable reason for invoking the right to self-defense, underscoring the complex relationship between state and non-state actors in the ever-evolving landscape of cyber warfare.[10]

---

[8] Nations, United. 'United Nations Charter (Full Text)'. *United Nations*, https://www.un.org/en/about-us/un-charter/full-text.

[9] Ministerie van Volksgezondheid, Welzijn en Sport. *Vigilance: Reporting Incidents and Corrective Actions - Medical Technology - Health and Youth Care Inspectorate*. 28 May 2021, https://english.igj.nl/medical-technology/market-supervision/vigilance-reporting-incidents-and-corrective-actions.

[10] 'ESCR Resources'. *ESCR-Net*, https://www.escr-net.org/resources/non-state-actors%2

Cyber Proxies

Cyberwarfare entails actions undertaken by nations or entities to target countries or institutions' computer networks. The goal is to disrupt, damage, or dismantle infrastructure through methods like computer viruses or denial-of-service attacks.[11]

Cyberattack

A cyberattack is defined as any deliberate attempt to steal, expose, alter, disable, or destroy data, applications, or other assets by gaining unauthorized access to a network, computer system, or digital device. The definition of a cyberattack underscores the essence of the Paradox of Progress, as it represents a dark side of technological advancement. In our interconnected world, the same networks and devices that enhance communication and productivity are vulnerable to deliberate attempts to breach security, emphasizing the complex trade-offs that come with technological innovation. [12]

Principle Of Proportionality

The principle of proportionality, which states that even if an attack is permitted, it must not be disproportionate in comparison to the predicted military advantage, is a key idea in international humanitarian law.[13]

BACKGROUND INFORMATION

Casus Belli in the Cyber Domain: The Debate over "Armed Attack" and "Use of Force"

In the developing cyber landscape, the question of what constitutes Casus Belli, particularly in relation to "armed attack" and "use of force", has become a highly debated topic in international relations and cyber security circles. As states grapple with the complexities of cyberwar, the definitions of these terms have important implications for the application of international law, particularly the right to self-defense.

Article 51 of the United Nations Charter enshrines the right to self-defense in the event of an "armed attack." To distinguish between conventional and cyber warfare, consider the 2001 U.S. response to the 9/11 terrorist attacks. Here, the U.S. invoked Article 51 to justify self-defense against Al-Qaeda, a non-state actor responsible for physical attacks. This example underscores the traditional interpretation of self-

[11]Cyber Warfare Pelechrinis, Konstantinos, et al. 'Denial of Service Attacks in Wireless Networks: The Case of Jammers'. *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, 2011, pp. 245–57. *DOI.org (Crossref)*,

[12] *What Is a Cyberattack? | IBM*. https://www.ibm.com/topics/cyber-attack

[13] 'The principle of proportionality'. *Diakonia International Humanitarian Law Centre*, https://www.diakonia.se/ihl/resources/international-humanitarian-law/ihl-principle-proportionality/

defense against tangible armed assaults by non-state actors. However, defining what constitutes an "armed attack" in cyber warfare remains a complex issue, emphasizing the challenges in applying Article 51 to the digital age. However, in the context of cyberspace, defining what constitutes an "armed attack" remains elusive and contentious. The ambiguity arises from the difficulty in attributing cyber incidents to specific state actors and distinguishing between hostile cyber activities and cyber-espionage.

Some countries debate the traditional interpretation of "armed attack", arguing that it should only include cyber incidents that cause physical damage or casualties similar to military attacks. This view emphasizes the importance of maintaining the principle of proportionality in safeguard measures. It contends that cyberattacks ought to be considered an "equipped assault" in the event that they result in physical harm or casualties comparable to customary military assaults.

Unlike “armed attack”, the concept of “use of force” in cyberspace is broader and includes more cyber activities. The UN Charter does not explicitly define the "use of force", which further complicates its interpretation in cyberspace. Some states assert that the threshold for "use of force" should mirror the traditional concept used in the physical realm. They argue that only cyber operations with significant destructive capabilities or those directly targeting critical infrastructure should qualify as a "use of force." On the other hand, many are the ones who believe that information warfare and influence operations should be considered "use of force" when they aim to undermine a nation's sovereignty, stability, or democratic processes, as they argue that such actions can be as detrimental as physical force. In the realm of cyberspace, the interpretation of the term "use of force" is a point of contention, extending beyond the traditional concept of "armed attack."

International Law and the Challenges of Establishing Universal Definitions of Casus Belli in Cyberspace

There are many factors that make it challenging to define what constitutes an armed attack in the cyberspace. Firstly, unlike traditional armed attacks with a clear threshold of intensity, cyberattacks vary in scale and impact. Some cyber problems can cause minimal disruption, while others can lead to widespread damage. Determining where the line is drawn between cyber incidents of varying degrees and those that qualify as armed attacks requires nuanced factors.

Attributing cyberattacks to specific state actors remains one of the most significant challenges in establishing universal definitions for armed attacks in cyberspace. The anonymous and deniable nature of cyber operations often makes it difficult to conclusively determine the responsible party. This lack of attribution complicates the application of international law and the potential invocation of self-defense measures.

Cyberattacks orchestrated by non-state actors further complicate the process of defining armed attacks. These actors may be difficult to identify, and their motivations may vary widely. From harming some specific people, to harming whole countries' economies or military infrastructures.

The WannaCry ransomware attack in May 2017 is a noteworthy example of an assault by non-state actors. This attack, which has been largely attributed to the North Korean hacker group Lazarus, affected over 230,000 systems in over 150 countries. WannaCry encrypted victims' files and demanded a Bitcoin ransom payment for their release by exploiting a vulnerability in obsolete Microsoft software. The attack brought key systems like healthcare, transportation, and public utilities to a halt. The attackers' goals were varied, covering both financial gain through ransom payments and geopolitical posturing. This example highlights the blurring lines between state and non-state actors in the cyber domain. It's difficult to define an act of war when an attack is carried out by a non-state group, even if it's believed to be acting on behalf of a nation.[14]

Another example is the cyber espionage outfit APT29, often known as Cozy Bear. This outfit has been linked to various high-profile cyber campaigns and is suspected of having ties to the Russian government. In 2015 and 2016, one significant operation involved accessing the Democratic National Committee's (DNC) networks. The goal of this breach was thought to be the capture and eventual distribution of sensitive political material in order to affect the United States presidential election. The attack highlighted non-state actors' ability to influence political processes and stir division on a global scale. The operation's goal was to influence the U.S. presidential election by stealing and potentially releasing sensitive political material. This demonstrates how non-state actors can use cyber means to influence political processes and potentially destabilize nations, creating a challenge in determining the threshold for Casus Belli in the cyber realm.[15]

One of the most significant challenges in cyberspace is the difficulty in attributing cyberattacks to specific perpetrators. The anonymity and agility afforded by the digital environment make it challenging to identify responsible actors accurately. This complicates the application of the right to self-defense, as a nation must determine who the aggressor is before taking any retaliatory action. Attributing cyberattacks to specific state or non-state actors is a central challenge in the realm of cybersecurity and international relations.

[14] 'What is WannaCry ransomware?' *www.kaspersky.com*, 6 July 2023, https://www.kaspersky.com/resource-center/threats/ransomware-wannacry.
[15] Braw, Elisabeth. 'Cyberattacks Are on the Decline'. *Foreign Policy*, 6 Feb. 2024, https://foreignpolicy.com/2020/12/16/cyberattacks-are-on-the-decline/.

Cyber attackers often use sophisticated techniques, such as using multiple layers of proxies and masking their origins, to conceal their identities. These methods make it difficult to directly attribute network incidents to a particular actor.

Malicious actors can conduct fake flagging operations that mimic the tactics, techniques and processes of other entities to deflect blame and create confusion. Misallocation can lead to unintended escalation and exacerbate tensions between countries. Involvement of non-state actors or state-sponsored cyber operations adds another layer of complexity to attribution challenges. Non-state actors can act independently or on behalf of the state, resulting in, most of the times, malicious activities.

The Application of the Right to Self-Defense in Cyberspace

The right to self-defense, enshrined in Article 51 of the United Nations Charter, is a fundamental principle of international law. As the field of cyberspace becomes increasingly important in the digital age, questions regarding how the right to self-defense applies in this area have arisen.

Attributing cyberattacks to specific state actors is a significant hurdle in applying the right to self-defense in cyberspace. The anonymous and sophisticated techniques used by cyber adversaries make it challenging to accurately identify the perpetrators. Moreover, the principle of proportionality adds another layer of complexity to determining the appropriate response to a cyber incident. The principle of proportionality is central when assessing responses to cyberattacks and determining the appropriateness of self-defence measures. Nations have the right to protect themselves through various means, including digital and physical responses. However, the threshold for justifying a conventional military reaction to a cyberattack is set quite high, typically requiring the cyber incident to be on a scale, impact, and with an intent resembling an armed attack. The challenge of establishing when a cyberattack qualifies as an armed attack, especially due to difficulties in attribution, adds complexity to this issue. International standards and frameworks, such as the Tallinn Manual and the work of the UN Group of Governmental Experts, seek to offer guidance and clarity in addressing these intricate aspects of cyber conflict. They aim to ensure that responses, whether in cyberspace or through conventional military actions, align with the principle of proportionality and international law while effectively protecting national interests.

The right to self-defense in cyberspace raises questions about the scope and nature of the measures permitted. Unlike traditional warfare, where boundaries and territories are clearly defined, cyberspace operates across geographic borders.

The Situation Today

The global threat environment has evolved, with cyberattacks being increasingly used by state and non-state actors. Recent events, such as the conflict in Ukraine, have shown that cyberattacks can be wielded as part of broader geopolitical strategies. This underscores the importance of clearly defining when a cyberattack qualifies as an armed attack, as these incidents can escalate into real-world conflicts.

While there are some international norms addressing cyber conflict, their interpretation remains a topic of debate. Documents like the Tallinn Manual offer guidance on international law in cyberspace, but they lack legal binding. Furthermore, the United Nations Group of Governmental Experts has made efforts to address responsible state behaviour in cyberspace but has yet to produce a universally accepted framework. The lack of consensus on the threshold for considering a cyberattack an armed attack complicates effective responses and creates uncertainty.

The international community is now urged to tackle the challenges posed by cyber conflicts. It is imperative to establish clear definitions and norms for Casus Belli in cyberspace. This includes determining the criteria for when a cyberattack is considered an armed attack, methods for attributing these attacks, and appropriate responses, which may encompass both digital and physical measures. Moreover, addressing the accountability of state and non-state actors engaged in cyber aggression is crucial.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

Australia

Australia holds that the thresholds and restrictions limiting the use of self-defense apply to both cyberattacks that qualify as armed attacks and self-defense actions that are carried out using cyberspace. Therefore, the fundamental right to self-defense is invoked if a cyber activity, whether conducted alone or in conjunction with a physical operation, causes damage or poses a serious threat of causing damage comparable to a traditional armed attack. Any use of force in self-defense must be required to fend off an actual or impending armed attack and must be proportionate in terms of time, breadth, and power.[16]

Brazil

There is no right to self-defense regarding cyberattacks in Brazil whenever there is not a real or impending armed attack. Finally, self-defense against armed attacks brought

[16]Brandis QC, Attorney-General of Australia, Senator the Hon. George. 'The Right of Self-Defence Against Imminent Armed Attack In International Law'. *EJIL: Talk!*, 25 May 2017, https://www.ejiltalk.org/the-right-of-self-defence-against-imminent-armed-attack-in-international-law/.

on by digital means must be necessary and reasonable, just like responses to armed operations involving conventional weapons.[17]

Canada

Canada believes that the natural right to self-defense in the event of an armed attack against a State also applies online. Canada's National Cyber Security Strategy outlines the country's approach to enhancing cybersecurity. It focuses on protecting critical infrastructure, fostering innovation, and collaborating with various stakeholders to ensure a secure digital environment.

Canada has faced several high-profile data breaches, including the 2019 Capital One breach that exposed the personal information of millions of Canadians. These incidents highlight the need for robust data protection measures. Canada, in response, tried to furtherly enhance its data protection systems by investing more money to its secret forces.[18]

China

China's stance on the right to self-defence in cyberspace is characterized by a certain level of ambiguity. Despite not having articulated a specific and comprehensive position, it has demonstrated reluctance towards endorsing a broad interpretation of the right to self-defence, particularly when no armed attacks are involved. This caution could be attributed to apprehensions linked to China's own history of alleged cyberattacks against other nations. Embracing a more expansive right to self-defence could potentially subject China to international legal ramifications and countermeasures. Furthermore, this stance allows China to steer clear of potential legal constraints on its own cyber operations, and it aligns with its strategic interests in shaping global cyber norms to suit its national security objectives. This position underscores the intricate and challenging nature of establishing international norms in the ever-evolving cyberspace arena, as states seek to balance their individual interests and security considerations in this dynamic landscape.[19]

France

Fully obeying Article 51 of the United Nations Charter, France holds the view that a State that suffers an armed attack is entitled to use individual or collective self-defense. Self-defense in response to an armed attack carried out in cyberspace may involve digital or conventional means in compliance with the principles of necessity and proportionality. On a decision by the President of the Republic to commit the

[17] Moorehead, Alex. 'Brazil's Robust Defense of the Legal Prohibition on the Use of Force and Self Defense'. *Just Security*, 20 Apr. 2018, https://www.justsecurity.org/55126/brazils-robust-defense-legal-prohibition-force/.

[18] OIU Robert H. McKinney School of Law: IUPUI'. *IU Robert H. McKinney School of Law*, https://mckinneylaw.iu.edu/error/404.html.

[19] Daum, Jeremy. 'Standing Your Ground, China Style'. *China Law Translate*, 5 Oct. 2020, https://www.chinalawtranslate.com/standing-your-ground-china-style/

French armed forces, the Armed Forces Ministry may carry out cyberoperations for military purposes in cyberspace. However, such a measure has not been put in place considering the fact that there wasn't a case where it could be used.[20]

Germany

Germany has called for a rules-based order in cyberspace, emphasizing the importance of norms and cooperation to ensure stability and security. The response to malicious cyber operations constituting an armed attack, is not limited to cyber counter-operations. Once the right to self-defense is triggered, Germany can resort to all necessary and proportionate means in order to end the attack. Self-defense does not require using the same means as the attack which provided the trigger for its exercise. [21]

Russian Federation

The Russian Federation emphasizes the principles of sovereignty, non-interference, and respect for each country's territorial integrity in cyberspace. Although how "hypocritical" this statement may sound, Russia in practice had several times conducted cyberattacks against their rivals. For example, including during the conflict in Eastern Ukraine and the annexation of Crimea, Russia has been accused of initiating cyberattacks against Ukraine. Systems used by the Ukrainian government, vital infrastructure, and energy plants have all been the targets of these attacks. Russia upholds the importance of multilateral cooperation to address cybersecurity challenges and believes that international law, including the United Nations Charter in Article 51, should be applied in cyberspace. Concluding, Russia believes that a country has the right to self-defend itself if the cyberattack threatens the country's sovereignty.[22]

United Kingdom (UK)

The United Kingdom believes that if a country's sovereignty is threatened via a cyberattack, the victimized country should reply. For example, the UK holds the view that if a hostile state interferes with the operation of one of their nuclear reactors, resulting in widespread loss of life, the fact that the act is carried out by way of a cyber operation does not prevent it from being viewed as an unlawful use of force or an armed attack against them, thus, enabling them to use the right to self-defense. This is why they are currently trying to implement the Active Cyber Defense (ACD) program, which automatically prevents cyberattacks on United Kingdom's

[20] *The Military Response to ISIS: A Historical Perspective | History Today*. https://www.historytoday.com/military-response-isis-historical-perspective.
[21] *The Military Response to ISIS: A Historical Perspective | History Today*. https://www.historytoday.com/military-response-isis-historical-perspective.
[22] Schmitt, Michael N. "Russia's 'Special Military Operation' and the (Claimed) Right of Self-Defense." *Lieber Institute West Point*, 20 Mar. 2023, . https://lieber.westpoint.edu/russia-special-military-operation-claimed-right-self-defense/

parliamentary systems and the wider public sector. It includes initiatives like the "Protective Domain National Service (PDNS)", which blocks access to malicious websites and helps prevent users from inadvertently interacting with cyber threats. [23]

United States (US)

The United States has for a long time taken the position that the inherent right of self-defense potentially applies to any illegal use of force. In their view, there is no threshold for the use of deadly force to qualify as an "armed attack" that may warrant a forcible response. But that is not to say that any illegal use of force triggers the right to use any and all force in response—such responses must still be necessary and, of course, proportionate. A past event that the US has tackled by preventing it from happening is "the Moonlight Maze," as it was one of the earliest known incidents of state-sponsored cyber espionage and involved a series of cyber activities targeting U.S. government agencies and defense contractors. The operation highlighted the potential for digital attacks to compromise national security and the sensitive information of millions of people.[24]

European Union Agency for Cybersecurity (ENISA)

Like many international organizations and cybersecurity authorities, ENISA has historically prioritized robust cybersecurity practices, incident response, and collaboration in order to thwart and lessen cyber threats. The focus is frequently on preventative actions, including risk assessment, exchanging threat intelligence, incident reporting and developing strong defense systems.

The ECSM is an annual campaign that is being held in October and aims to raise awareness about cybersecurity dangers, promote cybersecurity practices, and provide valuable information for citizens and businesses to enhance their online security. The program consists of various activities, workshops, and events throughout the 27 countries of the European Union, contributing to a safer digital environment.

United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Telecommunications in the Context of International Security

The United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Telecommunications in the Context of International Security is a key player in shaping international norms for cyberspace. It highlights that established international laws, such as the United Nations Charter, are relevant in the digital domain. This means that the fundamental principles governing state sovereignty, non-

[23] O'Meara, Christopher. "Necessity and Proportionality and the Right of Self-Defence in International Law." *UCL Discovery - UCL Discovery*, UCL (University College London), 28 Oct. 2018, discovery.ucl.ac.uk/id/eprint/10057299/.

[24] Vindman, Yevgeny. "Is the Solarwinds Cyber Attack an Act of War? It Is, If the United States Says It Is." *Default*, 26 Jan. 2021, www.lawfaremedia.org/article/solarwinds-cyberattack-act-war-it-if-united-states-says-it.

interference, and peaceful conflict resolution should also apply to the online world. In essence, it asserts that the same rules that guide how states behave and interact in the physical world should guide their actions in the virtual world. By emphasizing this continuity, the UN GGE promotes a structured approach to cybersecurity, establishing a framework for responsible state conduct in cyberspace to enhance global stability and security. This mirrors the broader effort to ensure that nations uphold established international norms and principles when operating and interacting in the online realm, much like they do in the physical world.

TIMELINE OF EVENTS

DATE	DESCRIPTION OF EVENT
November 3, 2010	Stuxnet, a cyberweapon allegedly developed by the United States and Israel, targets Iran's nuclear program, successfully sabotaging uranium centrifuges, causing physical damage to Iran's nuclear facilities; many argue that this should be deemed an “armed attack”.
February 4, 2013	The Tallin Manual is published, a comprehensive analysis of how international law, including the law of armed conflict, applies as regards cyber operations.
February 2, 2017	Tallin Manual 2.0 is published as a guide on how the already existent Tallin Manual applies to cyberspace.
June 28, 2017	NotPetya, a ransomware attack initially targeting Ukraine that later spreads globally, affects numerous multinational corporations, and causes billions of dollars in damages; many argue that this should be deemed an “armed attack” due to its extensive economic impact.
March 25,2003	Titan Rain, a series of continued cyberattacks targeting US defense bases and government agencies, highlights the vulnerability of sensitive national security information and underscores the need for robust cybersecurity measures to protect critical defense infrastructure and classified data, leading to increased investment in cyber defense capabilities.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

Tallinn Manual

The "Tallinn Manual" is a comprehensive analysis of how international law, including the law of armed conflict, applies to cyber operations. Drafted by legal experts on 2013 and published by the North Atlantic Treaty Organization (NATO) Cooperative

Cyber Defense Centre of Excellence in 2017, it offers guidance on cyberwarfare, self-defense, and other legal aspects in cyberspace. Due to this, NATO countries are now, more than ever, getting prepared and educated on the matter of cyber warfare and the dangers that lie beneath. Although it's not legally binding, it's of a great significance.

Tallin Manual 2.0

Officially titled "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" represents a significant previous attempt to address the challenges surrounding international law and cyber operations. It was the second edition of the Tallinn Manual, produced by the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), and aimed to provide guidance on how existing international law principles apply to cyberspace. Overall, Tallinn Manual 2.0 represented a significant step forward in attempting to address the complexities of international law in the context of cyber operations. Tallinn Manual 2.0, while offering valuable insights into Casus Belli and the right to self-defence in the context of cyber operations, lacks a universally accepted standard for defining an armed attack in cyberspace. Its definitions of "physical harm" and "destruction" remain somewhat ambiguous, leaving room for differing interpretations among nations. Moreover, the manual does not extensively address the intricate issues of attribution and intent, both of which are pivotal in accurately identifying the origin and purpose of a cyber operation.

Paris Call for Trust and Security in Cyberspace

Launched in 2018, the Paris Call is an initiative that aims to establish a framework for responsible state behavior in cyberspace. It calls for adherence to certain principles, including not attacking critical infrastructure or interfering with electoral processes. This Call for Trust (CfT) is of great importance, and it can be proven very beneficial as well, mainly since it shows that under no circumstances should humans treat civilians in an inhumane way. While it does not explicitly define what constitutes an armed attack in the digital realm, the initiative seeks to prevent the escalation of conflicts by calling for the safeguarding of critical infrastructure and the non-interference with electoral processes. By fostering trust, responsible conduct, and adherence to international norms and principles, the Paris Call contributes to a more stable and secure cyberspace, reducing the risk of cyber actions that might trigger the right to self-defense.

POSSIBLE SOLUTIONS

International standards and Agreements

Promoting the creation of international standards and agreements that apply across borders to regulate state behavior in cyberspace is a crucial step toward enhancing cybersecurity, fostering stability, and preventing misunderstandings and unintended

escalations. Developing clear thresholds and expectations for state conduct in cyberspace can lead to increased trust, transparency, and cooperation among nations. Creating international standards and agreements for cyberspace will require concerted efforts from the international community. Key steps to achieve this solution include Multilateral Dialogue and the possible creation of a Cybersecurity Coalition between the member states of the UN.

Strengthening Cybersecurity Cooperation

Strengthening international cybersecurity cooperation is a pivotal strategy that holds relevance for the Casus Belli issue in cyberspace. Collaborative efforts and information sharing among nations can significantly reduce the risk of misattribution, mitigating the potential triggers for self-defence claims. Enhanced threat intelligence exchange and swift incident response, possibly coordinated through organizations like INTERPOL, enable countries to collectively understand, manage, and respond to cyber incidents. Through these collaborative cybersecurity measures, nations can create an environment where the threshold for Casus Belli is less likely to be crossed due to misunderstandings, ultimately bolstering stability and security in the digital realm. This cooperative approach not only safeguards against cyber threats but also serves to prevent unintentional escalations that could lead to armed conflicts in cyberspace.

Improved Transparency

Improving cybersecurity transparency is key to building trust between countries, enhancing global cyber stability and reducing the risk of misunderstandings and unintended escalation. By promoting openness and honesty about their cyber capabilities and intentions, countries can promote a safer and more cooperative cyberspace under the realms of INTERPOL. This can be achieved by requiring private sector entities to be more transparent about their cybersecurity practices and so contribute to overall cyber stability. And by embracing participation in discussions, like the ENISA program on international norms and standards for responsible state behavior in cyberspace which can foster not only transparency but also accountability.

Dispute Resolution Mechanisms

Dispute resolution mechanisms can play an important role in preventing or de-escalating cyber conflicts between countries. Establishing effective mechanisms for resolving cybersecurity disputes can prevent tensions from escalating into full-blown cyber confrontations and promote stability in cyberspace. Such mechanisms can be achieved by encouraging countries to voluntarily participate in dispute resolution mechanisms such as open dialogues with result of enhancing their legitimacy and effectiveness.

BIBLIOGRAPHY

The _____ of the English Defines “cyberspace” as the Notional Environment in Which Communication over Computer Network Occurs.BE’s New DictionaryOxford DictionaryUrban DictionarySamuel Johnson’s Dictionary’. *Toppr Ask*, https://www.toppr.com/ask/question/the-of-the-english-defines-cyberspace-as-the-notional-environment-in-which-communication-over/.

Self-Defence | How Does Law Protect in War? - Online Casebook. https://casebook.icrc.org/a_to_z/glossary/self-defence.

Perpetrator. 31 Jan. 2024, https://dictionary.cambridge.org/dictionary/english/perpetrator.

Espionage. 31 Jan. 2024, https://dictionary.cambridge.org/dictionary/english/espionage.

Ministerie van Volksgezondheid, Welzijn en Sport. *Vigilance: Reporting Incidents and Corrective Actions - Medical Technology - Health and Youth Care Inspectorate*. 28 May 2021, https://english.igj.nl/medical-technology/market-supervision/vigilance-reporting-incidents-and-corrective-actions.

‘ESCR Resources’. *ESCR-Net*, https://www.escr-net.org/resources/non-state-actors%2

Cyber Warfare Pelechrinis, Konstantinos, et al. ‘Denial of Service Attacks in Wireless Networks: The Case of Jammers’. *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, 2011, pp. 245–57. *DOI.org (Crossref)*,

What Is a Cyberattack? | IBM. https://www.ibm.com/topics/cyber-attack

The principle of proportionality’. *Diakonia International Humanitarian Law Centre*, https://www.diakonia.se/ihl/resources/international-humanitarian-law/ihl-principle-proportionality/

What is WannaCry ransomware?’ *www.kaspersky.com*, 6 July 2023, https://www.kaspersky.com/resource-center/threats/ransomware-wannacry.

Braw, Elisabeth. ‘Cyberattacks Are on the Decline’. *Foreign Policy*, 6 Feb. 2024, https://foreignpolicy.com/2020/12/16/cyberattacks-are-on-the-decline/.

Brandis QC, Attorney-General of Australia, Senator the Hon. George. ‘The Right of Self-Defence Against Imminent Armed Attack In International Law’. *EJIL: Talk!*, 25 May 2017, https://www.ejiltalk.org/the-right-of-self-defence-against-imminent-armed-attack-in-international-law/.

Moorehead, Alex. ‘Brazil’s Robust Defense of the Legal Prohibition on the Use of Force and Self Defense’. *Just Security*, 20 Apr. 2018, https://www.justsecurity.org/55126/brazils-robust-defense-legal-prohibition-force/.

OIU Robert H. McKinney School of Law: IUPUI'. *IU Robert H. McKinney School of Law*, https://mckinneylaw.iu.edu/error/404.html.

Daum, Jeremy. 'Standing Your Ground, China Style'. *China Law Translate*, 5 Oct. 2020, https://www.chinalawtranslate.com/standing-your-ground-china-style/

The Military Response to ISIS: A Historical Perspective | History Today. https://www.historytoday.com/military-response-isis-historical-perspective.

he Military Response to ISIS: A Historical Perspective | History Today. https://www.historytoday.com/military-response-isis-historical-perspective.

Schmitt, Michael N. "Russia's 'Special Military Operation' and the (Claimed) Right of Self-Defense." *Lieber Institute West Point*, 20 Mar. 2023, . https://lieber.westpoint.edu/russia-special-military-operation-claimed-right-self-defense/

O'Meara, Christopher. "Necessity and Proportionality and the Right of Self-Defence in International Law." *UCL Discovery - UCL Discovery*, UCL (University College London), 28 Oct. 2018, discovery.ucl.ac.uk/id/eprint/10057299/.

Vindman, Yevgeny. "Is the Solarwinds Cyber Attack an Act of War? It Is, If the United States Says It Is." *Default*, 26 Jan. 2021, www.lawfaremedia.org/article/solarwinds-cyberattack-act-war-it-if-united-states-says-it.