From Code to Conflict: Navigating Cyber Attacks and the UN Charter's Force Prohibition

من الشفرة إلى الصراع: التعامل مع الهجمات السيبرانية وحظر استخدام القوة في ميثاق الأمم المتحدة

Dr Ahmed Aubais alfatlawi

Prof of Public International law
University of Kufa: Faculty of Law
ahmeda.alfatlawi@uokufa.edu.iq

الدكتور احمد عبيس الفتلاوي
بروفيسور القانون الدولي العام بجامعة الكوفة / كلية القانون

الكلمات الافتتاحية :
الشفرة + الصراع + الهجمات السيبرانية +حظر استخدام القوة +ميثاق الأمم المتحدة

Keywords :
Code + Conflict + Cyber Attacks + Prohibition of the Use of Force + UN Charter

الملخص :في عصر القوة الرقمية، حيث يمكن أن تتحول الخوارزميات المعززة بالشفرة إلى سلاح، أصبحت مواءمة الهجمات السيبرانية مع حظر ميثاق الأمم المتحدة لاستخدام القوة تحديًا بالغ الأهمية. يتطلب التحول من ساحات المعارك المادية إلى الساحات الافتراضية منظورًا جديدًا لما يشكل "هجومًا مسلحًا" وكيف يمكن للمعايير القانونية الراسخة معالجة أشكال جديدة من العدوان. وبينما نتنقل عبر هذا التفاعل المعقد بين التكنولوجيا والقانون الدولي، من الواضح أن تفاني ميثاق الأمم المتحدة للسلام والأمن يحتاج إلى التكيف مع المشهد السيبراني. وعلى الرغم من أن دليل تالين يقدم إرشادات قيمة، إلا أنه لا يزال يتطور، وهو ما يؤكد على الصراع المستمر لتحديد وتنظيم الصراعات السيبرانية. لقد قسمت الدراسة إلى جزئين ، الأول يبحث في إطار قواعد

استخدام القوة وفقا لميثاق الأمم المتحدة والموقف من الهجمات السيبرانية، أما الثاني فبحث في مناهج ومعايير وصول الهجمات السيبرانية إلى عتبة استخدام القوة، وتوصلنا إلى نتيجة مفادها : أنه وفي حين يقدم ميثاق الأمم المتحدة إطاراً واسعاً لاستخدام القوة والدفاع عن النفس، فإنه يفتقر إلى إرشادات محددة للعمليات السيبرانية. ورغم أن دليل تالين يوفر تحليلاً أكثر تفصيلاً، فمن المهم أن نلاحظ أنه غير ملزم قانوناً. ويجب أن يتوصل المجتمع الدولي، فضلا عن إسهام فقهاء القانون إلى الآلية التي يمكن فيها تطبيق الأطر القانونية الراهنة و القائمة على الهجمات السيبرانية واستخدام القوة. يشير هذا الملخص إلى أن جوهر حظر القوة الوارد في الميثاق ، لا يكمن في أسلوب العدوان ولكن في الضرر الناجم عنه. و مع تزايد تعقيد الهجمات السيبرانية، يجب أن تتطور أطرنا القانونية لمواجهة هذه التهديدات الجديدة. وبعبارة أخرى أن نواجه التحدي المتمثل بالموازنة بين السلام الدولي والجوانب الفريدة للعمليات السيبرانية. ولمعالجة هذه التحديات، يتعين علينا تعزيز التعاون العالمي وتطوير معايير قانونية مرنة تأخذ في الاعتبار الطبيعة المتميزة للهجمات السيبرانية العدوانية. وهذا لا يتطلب الابتكار القانوني فحسب، بل يتطلب أيضا جهدا عالميا موحدا لفهم وتخفيف مخاطر الصراع الرقمي. ومن خلال سد الفجوة بين الأطر القانونية القائمة والتهديدات الحديثة، يمكننا أن نحافظ على روح ميثاق الأمم المتحدة في حين نتعامل بفعالية مع حقائق العصر الرقمي. ونخلص إلى أن الحظر المفروض على استخدام القوة بموجب المادة ٢(٤) من ميثاق الأمم المتحدة لا ينبغي أن يساوي الحق في الدفاع عن النفس بموجب المادة ٥١. والواقع أن المفهوم التقليدي للقوة الحركية يحتاج إلى إعادة تقييم، لأن التأثير الواسع والفوري للأساليب غير الحركية مثل الهجمات السيبرانية يمكن تكييفه أيضا هجوما مسلحا. واستجابة

للطبيعة المتطورة لاستخدام القوة، وخاصة في المجال الرقمي، يتعين علينا أن نلتزم بالسلام والأمن مع تبني الحلول التي تعالج الثغرات في المعايير القانونية الحالية. نقترح مبادرة بقيادة الأمم المتحدة لإنشاء اتفاقية دولية تحدد مدونة سلوك ملزمة للأنشطة السيبرانية، على أساس مبادئ ميثاق الأمم المتحدة الواردة في الفصل السابع. أن اقتراحنا ، يدمج ثلاثة عناصر رئيسة وهي: حظر القوة المسلحة في المادة ٢، الفقرة ٤ من ميثاق الأمم المتحدة، والاستثناءات للدفاع عن النفس في المادة ٥١، والمادة ٨ مكرر من النظام الأساسي للمحكمة الجنائية الدولية، والتي تتعامل مع جريمة العدوان. ومن خلال الجمع بين هذه العناصر، نسعى إلى إرساء استجابة عالمية واضحة وموحدة للتهديدات الغامضة للعدوان السيبراني، وضمان استراتيجية متماسكة لمعالجة تحديات القوة الرقمية.

Abstract

The two-part article delves into the challenge that cyberattacks present to the UN Charter's prohibition on using force and the associated exceptions. In the urgent era of digital warfare, where code can be wielded as a weapon, aligning cyberattacks with the UN Charter's prohibition on using force has emerged as a pressing challenge. The transition from physical battlefields to virtual arenas necessitates a fresh perspective on what constitutes an 'armed attack' and how established legal norms can confront new forms of aggression. This article will examine critical issues, such as what specific flexible legal norms should be developed to address cyber warfare's distinct nature.

How can global cooperation be enhanced to mitigate the risks of digital conflict effectively? What challenges might arise in establishing a clear and unified global response to the threats of cyber aggression through an international agreement? As we navigate this complex interplay between technology and international law, it's evident that the UN Charter's dedication to peace and security needs to adapt to the cyber landscape. Although the Tallinn Manual offers valuable guidance, it's still evolving, underscoring the ongoing struggle to define and regulate cyber conflicts. Our analysis indicates that the essence of the Charter's prohibition on force lies not in the mode of aggression but in the harm caused. As cyberattacks grow more sophisticated, our legal frameworks must evolve to meet these new threats. We face the challenge of balancing international peace with the unique aspects of cyber operations. To address these challenges, we must enhance global cooperation and develop flexible legal norms that consider the distinct nature of cyber warfare. This necessitates not just legal innovation but a concerted global effort to understand and mitigate the risks of digital conflict. By bridging the gap between existing legal frameworks and modern threats, we can uphold the spirit of the UN Charter while effectively tackling the realities of the digital age. We conclude that the prohibition on using force under Article 2(4) of the UN Charter should

not be equated with the right to self-defence under Article 51. The traditional notion of kinetic force needs reassessment, as the broad and immediate impact of non-kinetic methods like cyberattacks could also be deemed an armed attack. In response to the evolving nature of conflict, particularly in the digital sphere, we must be committed to peace and security while embracing solutions that address the gaps in current legal standards. We propose a United Nations-led initiative, a pivotal step, to create an international agreement defining a binding code of conduct for cyber activities, firmly grounded in the principles of the UN Charter. Our proposal integrates three key elements: the prohibition of armed force in Article 2, Paragraph 4 of the UN Charter, the exceptions for self-defence in Article 51, and Article 8 bis of the International Criminal Court's Statute, which deals with aggression. By combining these elements, we seek to establish a clear and unified global response to the ambiguous threats of cyber aggression, ensuring a coherent strategy to address the challenges of digital warfare.

Introduction: In accordance with public international law, the characterization of an act as aggression has traditionally hinged on concrete physical elements.[1] Nevertheless, the emergence of cyberattacks has redefined established concepts by substituting

physical means and their tangible effects with digital methods that still yield physical impact. Ongoing research aims to define cyber aggression and its correlation with regulations prohibiting the application of armed force. While it is widely accepted that paragraph (4) of Article 2 predates the widespread use of information technology, it prompts whether it can be legitimately applied to cyberattacks. Nils Melzer and other legal experts unequivocally assert that the current international legal framework should be utilized to address cyberattacks. Their firm stance is that cyberattacks must be recognized as acts of aggression under the United Nations Charter, which explicitly prohibits using force, irrespective of the methods employed, when such actions contravene the UN's fundamental goals and principles.[2]

In their 2013 report, the Group of Governmental Experts established by the UN General Assembly emphatically affirmed that international law, particularly the UN Charter, unquestionably applies to states' use of ICTs. This assertion is vital for preserving peace and stability and fostering an open, secure, peaceful, and accessible ICT environment.[3]

Concerning Article 2, paragraph 4 of the Charter of the United Nations and the potential classification of cyber attacks as acts of aggression, it is imperative to meet three distinct criteria:

1. An aggressive cyber attack must unequivocally be attributable to a state. Actions carried out independently by individuals or armed groups do not fall under state jurisdiction, even if they result in similar harm to that caused by an aggressive state.

2. A cyber attack must undeniably pose a threat or use force.

3. The threat or use of force must unambiguously fall within international relations.

When considering the first criterion, which addresses the origin and attribution of cyber attacks to states, the primary challenge lies in applying paragraph 4 of Article 2 in the context of cyber warfare. The general assumption is that a cyber attack is solely attributed to the aggressor state. However, the reference to "international relations" in paragraph 4 of Article 2 indicates that cyber attacks must not only be carried out by a state, but also directed against another state. Therefore, paragraph 4 of Article 2 does not prohibit the threat or use of cyber attacks against non-state actors, even when the attacks amount to the use of force – as long as such action does not impact another state's territorial integrity or political independence. Finally, to apply paragraph 4 of Article 2, a cyber attack must unequivocally pose a threat or involve the use of force.[4] In its 1996 advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, the ICJ linked the

legitimacy of threats to the legality of the simultaneous use of force.[5] In the matter at hand, we pose the question: Can cyber-attacks be deemed as the use of force within the scope of Article 2, paragraph 4 of the Charter of the United Nations? The Tallinn Manual unequivocally references the 1986 ruling of the ICJ in the case of Military and Paramilitary Activities in and against Nicaragua. In this landmark precedent, the court distinctly establishes a crucial criterion for assessing the threshold for the use of force. It emphasizes the importance of considering the scale and impact of military actions in determining whether they unequivocally amount to an armed attack.[6] According to the Tallinn Manual, cyber-attacks should be carefully assessed to determine if they constitute a use of force. Experts unanimously argue that cyber-attacks should not be excluded from this analysis, which revolves around whether the scale and effects of the cyber operation are similar to those of traditional kinetic attacks.[7] Assessing the gravity and severity of cyber behaviour is a complex task because it relies on intangible elements, such as digital directives. Legal experts assert that establishing a delicate balance between the severity of cyber behaviour and the level of legal rights protected is essential before deeming it severe enough to justify using force.[8] In our view, behaviours in the cyber domain should only be considered dangerous if

they have a broad, long-lasting, and significant impact. Legal experts are currently discussing how to manage cyber attacks within the armed forces due to the lack of a formal, internationally agreed-upon protocol for such situations. This debate heavily revolves around defining cyber power and evaluating the consequences of cyber attacks.[9] Different esteemed international law scholars have meticulously crafted the Tallinn Manual, a comprehensive set of guidelines for comprehending cyber attacks. This discussion will be organized into two distinct sections: the first segment will thoroughly cover the approaches used to describe cyber power, while the second will delve into the factors devised by Michael Schmitt and the Tallinn Manual to ascertain the scope and impact of hostile cyber operations. With this essential information in mind, we will thoroughly dissect the topic by breaking it down into two parts. The first part will focus on researching and analyzing the concept of cyber attacks and associated terms, coupled with a meticulous review of various models of cyber attacks. Subsequently, the focus will tenaciously shift towards researching the most contentious legal and political matters, explicitly concerning the methods and standards utilized to uncover the nature of cyber power.

Section I: The concept of cyber attacks : In this section, we will provide a clear and detailed explanation of cyber attacks and their associated

terminology. This understanding is essential to comprehend the subsequent content of this study. In the second part, we will define cyber attacks and explore some of the world's most dangerous cyber attack models through compelling case studies.

First: Cyber attacks and the associated terminology: "Cyber" comes from the Greek word "cybernetics," which means command or remote control. It refers to the science of control and reflects the concept of cyber attacks involving systems' remote manipulation and management.[10] In cybersecurity, Michael Schmitt describes cyber attacks as intentional and carefully planned actions carried out by a country to disturb or weaken an adversary's computer and information systems or to protect the information systems of the attacking country."[11] In the Pentagon's 2015 dictionary, a "cyber attack" is described as actions carried out in cyberspace that lead to uncontrolled visible effects. These effects can include degradation, disruption, or destruction within cyberspace or manipulation that disrupts the physical domain. Essentially, a cyber attack is considered a form of force." [12] In contrast, the Tallinn 2.0 Manual defines a "cyber attack" as " a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons, or material damage or destruction to the attacked target." [13] After carefully reviewing the

definitions provided, we are confident that this definition best corresponds to our understanding of cyber attacks. All the definitions mentioned above clearly indicate that cyberspace is the primary medium for cyber attacks. If space has become a battlefield, it unequivocally signifies that many of the decisive battles in the twenty-first century will occur here. Therefore, it is absolutely crucial for us to understand the nature of cyberspace. The 2015 U.S. Department of Defense Military Dictionary defines cyberspace as a critical global domain within the information environment. It comprises interconnected networks of information technology infrastructures and resident data, encompassing the Internet, communications networks, computer systems, and embedded processors and controllers.[14] In exploring the effects of cyberspace, the definition provided describes "cyberspace" as a computer or software, including any combination of software, firmware, or hardware designed to produce an effect in or through cyberspace." [15] The definitions may become restrictive in the future due to the ongoing advancements in digital and information technology. As a result, new methods may arise that do not fit within these definitions.

Due to the ongoing advancements in digital and information technology, the definitions may become restrictive in the future. As a

result, new methods may arise that do not fit within these definitions. It is essential to highlight specific terms that link crime to the digital space, including the following:

(a) Cybercrime: refers to illegal activities committed for financial gain or fame, such as creating malware, distributing child pornography, kidnapping for ransom, and providing mercenary services.[16]

(b) Cyber espionage: Cyber espionage is a powerful tool driven by the relentless pursuit of sensitive information rather than an immediate intent to cause harm. Often orchestrated by individuals or state-affiliated groups, it aims to secure decisive financial or strategic military advantages.[17]

(c) Cyber terrorism: Just like all forms of terrorism, the primary aim is to sow terror and manipulate individuals. Cyber terrorists wield the malevolent tools present in cyberspace as weapons against both cyber and physical targets.[18]

It's crucial to understand that no universally accepted definition of cyber warfare exists. However, some experts have tried to clarify the concept. For instance, Richard Clarke and Robert Kennackie define "cyberwarfare" as the actions of a state hacking into another state's computers or networks to cause significant damage. [19]

Jeffrey Carr describes it as "the art and science of fighting without fighting, of defeating an adversary without bloodshed."[20] Nevertheless, it's essential to reconsider that cyberwarfare won't

involve bloodshed. For example, a cyberattack on critical national infrastructure like the electrical grid connected to healthcare infrastructure could lead to loss of life by disrupting service delivery due to hospital power outages.

James Bryan defines cyber warfare as a critical extension of policy through actions taken in cyberspace by state or non-state actors significantly supported by the state. These actions pose a severe threat to the security of another state or are taken in response to a threat of serious aggression to state security, whether actual or perceived. "[21] Bryan emphasizes that cyber warfare represents a growing and crucial aspect of international relations, encompassing organized or state-orchestrated computer network attacks witnessed in instances such as those in Estonia (2007), Georgia (2008), and Iran (2010). The term "cyber warfare," often used interchangeably with "cyber attacks" and "cyber aggression," epitomizes the utilization of technological power in the domain of computer networks. This involves storing, sharing, and transmitting information over the Internet. Furthermore, this method of waging war has the potential to be as destructive as any other traditional kinetic means used during an armed conflict, with the capability to impact various sectors, such as disrupting weather patterns and disabling critical infrastructure like nuclear power plants.[22]

Katie Terrell Hanna, Kevin Ferguson, and Linda Rosenkrantz define cyber warfare as a computer- or network-based conflict involving politically motivated attacks by one state on another. In these types of attacks, actors in one state attempt to disrupt the activities of other organizations or states, particularly for strategic or military purposes and cyber espionage."[23] Corniche proposes a different perspective on cyber warfare: "...It encompasses conflicts between states and the involvement of non-state actors. Targeting with proportionate force in cyberspace is challenging. The target could range from military or civilian entities to a server room hosting multiple customers, including the intended target".[24] This definition suggests that non-state actors could be involved in cyberattacks. The words "can" and "different methods" make it a more general and helpful definition. It highlights that cyberattacks can be unpredictable in medium or method, and their effects can be inaccurate, limiting the type and quantity of impact. This is an exciting idea that is missing in other definitions.[25] Cameron Peel defines "cyber aggression" as " the utilization of computer or internet technology to disrupt or harm a state's ability to function through economic, infrastructural, or political means, including invasive information warfare if it can be directly attributed to state actors".[26] He further argues that if it is proven that an act originated from private

individuals within a state, that state is responsible for capturing and prosecuting those individuals. Suppose a state fails to help capture and convict an individual proven to be involved in a cyber-attack. In that case, that state will be considered as aiding or encouraging such an attack. It would then be liable to lawful reprisals such as economic sanctions and monetary compensation to the victim state. These actions would be subject to proceedings in the International Court of Justice. Though this definition may not cover all scenarios, it is designed to evolve alongside computer and internet technology advances, while also addressing the current issue of direct connections to State actors.[27] With discussions in legal scholarship about the definition of "cyber" and the use of force, particularly in the context of cyber warfare and cyberterrorism, Jonathan A. Ophardt argues that the definition of a cyber attack is currently inconsistent and subject to varying interpretations. Some experts use the term to encompass a wide spectrum of cyberterrorism and cyberwarfare, while others differentiate cyberattacks as a distinct category. Furthermore, there is disagreement among experts on the criteria for classifying cyberwarfare, including whether it requires the simultaneous use of conventional weapons or should be assessed based on the attackers' identity and motives. Some also consider the type of targets and

degree of damage caused by the attacks. While it is widely acknowledged that Georgia was the victim of organized cyberattacks, there is debate regarding whether these attacks constituted cyber warfare.[28] We argue that The debate surrounding the definition of a cyberattack emphasizes the need to focus on the impact it produces. One perspective contends that if a cyberattack is comparable to using kinetic weapons, it should be considered an armed attack within the meaning of Article 49, paragraph (a) of Additional Protocol I of 1977. Navigating the complexities of cyberattack response under international law is a pressing challenge, given the dynamic nature of digital technology and its interaction with legal provisions. [29] In this regard, determining the severity of an attack in real-time and distinguishing between cyber activities in times of peace and those during armed conflict requires astute analysis and discernment.

In ancient times, disguise and deception were used in warfare. Some scholars argue that leaders have used deception throughout history to conceal their capabilities, maneuvers , and intentions, effectively denying their opponents situational awareness. This approach has consistently proven effective in achieving success on the battlefield.[30] Cyber hackers can swiftly adapt and unleash devastating attacks in today's interconnected world. This demands decisive and rapid

defensive measures. Network defence strategies must effectively combat both low- and high-risk threats, presenting a considerable challenge in making informed choices for self-protection.[31]

In today's world, cyber warfare has become a crucial element of armed conflict. Cyber attacks can have devastating effects on nations during both peacetime and war. The impact of cyber attacks is particularly significant during times of peace. Covert cyber attacks in times of peace can pose serious risks, especially for countries that lack the technological capabilities to detect or investigate them. For example, if a country experiencing severe electricity shortages fails to recognize a sustained cyber attack on its electricity sector, it could lead to domestic tensions, worsen economic challenges, and potentially spark civil unrest or revolution, causing destabilization within the country. In the context provided, cyber warfare is narrowly defined as using cyber technologies in armed conflicts.[32] Cyber attacks, in contrast, encompass a broader scope and can extend beyond formal wars, potentially catalyzing the initiation of armed conflict.[33]

Second: Examples of cyber attacks: To underscore the gravity of cyberattacks, one must consider instances such as those in Estonia in 2007, Georgia in 2008, Iran in 2010, and Ukraine in 2022. These cases have resulted in substantial consequences, including the outbreak of

armed conflicts, such as the conflict between Russia and Georgia, and the disruption of Estonia's internet communication and government departments. Furthermore, breaches of facility systems have occurred, notably the manipulation of protection systems for nuclear installations in Iran. These incidents constitute a significant threat to national security and international peace. The examples we will mention are but are not limited to, as many legal studies have been exposed to them.[34] Now, let's explore some examples and carefully assess them within the context of international regulations.

A- Cyberattack on Estonia (2007) : The 2007 cyber attacks on Estonia are a telling example, not only for being the first and attention-grabbing but also because Estonia is one of the world's most advanced countries in information technology. Estonian online banking transactions amounted to 97%, and in 2007, 60% of the population used the internet daily. The country's heavy reliance on technology made it particularly vulnerable to cyber-attacks. This is a stark reminder that the more interconnected a country's electronic infrastructure networks are, the more susceptible it becomes to cyber attacks.[35] The Estonian government has stated that the cyber attacks commenced on April 27, 2007, in response to the decision to relocate a monument from the former Soviet era in Tallinn. The attacks persisted for several weeks, at least until May 18, 2007, and even after this date, some small cyber

attacks were detected. Most of the attacks were aimed at denial of service (DDoS), specifically targeting various vital government institutions and disrupting essential public sector operations.[36] Estonia faced significant isolation at the time, with Internet banking and ATMs suspended and emergency communication services briefly interrupted. This upheaval led to widespread social and economic unrest, highlighting the critical importance of these services to society's functioning.[37] The series of events surrounding the cyber attacks in Estonia is as follows: Although Estonian emergency response teams effectively managed to contain the situation and prevent the worst possible outcome, where hackers took control of Estonian websites and posted the message "Hackers have been hacked," Estonia accused the Russian side of orchestrating the attacks. Estonia stated that the Russian side did not cooperate in helping to identify the trustworthy source of the attacks.[38] The Estonian government swiftly took action, leading to the apprehension of a Russian student in Tallinn for computer hacking. Symbolic fines were imposed as a consequence.[39] Estonia requested a bilateral investigation with Russia under their Mutual Legal Assistance Treaty, but the Russian prosecutor's office refused to assist previous promises.[40] Estonia accused Russia of sponsoring cyber attacks, but due to inconclusive investigations and Russia's denial of involvement, it lacked evidence to trigger international responsibility.[41] In the 1949 NATO Convention, Article 5 required the Alliance to

respond to any attack against a member state, which was considered an attack against all. If NATO fails to act, member states can use self-defence as outlined in Article 51 of the UN Charter.[42] In response, NATO established the Cyber Defense Cooperative Centre of Excellence (CCD COE) on May 14, 2008.[43] Based in Tallinn, Estonia, the centre is committed to strengthening NATO's rapid response to cyber-attacks through thorough attack analysis while also serving as a crucial platform for cyber defence education, research, and development.[44]

B- Cyber attack on Georgia (2008) : In 2008, Georgia conflicted with Russia over the disputed regions of Abkhazia and South Ossetia. Russia supported their independence, while Georgia sought to keep control.[45] Cyber attacks against Georgia began on July 20, 2008, a month before Russia used kinetic conventional military force, while denial of service (DDoS) attacks was widespread and led to the closure of most Georgian servers.[46]

On 7 August 2008, tensions over South Ossetia, in particular, increased: while Georgia claimed that South Ossetian rebels were firing rockets at Georgia, Russia claimed at the same time that a number of its peacekeepers had been killed, and in a swift reaction, on Russia 8 August 2008, sent tanks across the border with Georgia and launched air strikes against elected military targets.[47] Before the Russian invasion of Georgia in August 2008, large-scale cyberattacks disrupted

Georgian websites, including those of banks and ministries. These attacks contributed to the chaos of the conflict, known as the "fog of war".[48] The Russian government most likely orchestrated the attack to further its political and military goals in the crisis. However, it was loosely carried out by independent hackers, reinforcing the Russian government's denial of responsibility for these attacks in Georgia.[49] The cyber attacks on Georgia in 2008 were attributed to the organization RBN, which is affiliated with organized crime and based in St. Petersburg, Russia. Comprised of former KGB agents, RBN specializes in spyware, spam operations, web-based attacks, phishing, and innovative malware to control computers for recruitment into robot networks.[50]

Similar to the 2007 attacks against Estonia, there existed compelling circumstantial evidence implicating Russia's support and direction of the RBN in the attack on Georgia. However, the evidence again fell short of conclusively establishing international responsibility for aggression or individual criminal liability.[51] The cyber attacks on Georgian banks and government websites were unprecedented, as they were the first to be combined with traditional armed force. This has fundamentally changed the threat landscape for states relying on

computing and networks for trade, citizen communication, and critical infrastructure.[52]

C. Attack on Iran by Stuxnet : In 2010, a Belarusian information technology security company made a groundbreaking discovery. They uncovered a highly sophisticated virus known as Stuxnet, which sent shockwaves through the world of software security. This virus was used in a targeted attack on the nuclear facilities in the Iranian city of Bushehr.[53] Despite ongoing efforts, the official confirmation of the attack's source remains elusive. However, strong and compelling reasons exist to believe that the responsible party will be revealed.[54] Despite the United States and Israel denying any joint involvement in the attack using the Stuxnet virus, some data referenced the internal code name of the US government for the operation as "Olympic Games." The goal of the operation was to disable the Natanz nuclear reactor in the Iranian port of Bushehr.[55] According to experts in information technology, the Stuxnet virus employed an extremely aggressive strategy by exploiting a previously unknown vulnerability in Microsoft's systems, which Microsoft later confirmed. The virus targeted centrifuge controllers, injecting them with penetration code to manipulate the rotation speed of the centrifuges. Additionally, the virus deceived the private digital security system by using devices to provide readings that appeared normal while actively sabotaging the target system.[56] The most serious criminal proof is that the Stuxnet virus

would have destroyed itself and disappeared completely on June 24, 2012, with the virus trace smoothly erased from every infected device without being re-detected. [57] We believe that Stuxnet was a significant moment that highlighted the importance of understanding cyberattacks and adapting defence strategies in accordance with international law. This sophisticated program is unique in its ability to carry out precise and targeted cyberattacks without direct military involvement. It may represent a new form of hybrid warfare, effectively integrating cyber programs and kinetic energy-based weapons. In addition to the above, it was the only attack that caused significant physical destruction, although it was aimed at technical equipment.[58] The Stuxnet attack lasted almost seven years, from November 2005 to June 2012. The primary attack is believed to have occurred between June 2009 and June 2010, coinciding with the initial public reports by IT security firms.[59]

By the close of 2010, the virus had penetrated nearly 100,000 hosts in numerous countries, with a significant 60% directed at targets in Iran.[60] The most perilous targeting mechanism involved a highly intricate sabotage strategy aimed at undermining the operators of the protection programs at targeted facilities, notably the Iranian Natanz nuclear reactor. This was achieved by significantly prolonging the enrichment process. While some details and facts about the attack have been verified, the precise workings of the Stuxnet hacking technology

remain in mystery. [61] According to expert analysis, the Stuxnet virus is hailed as the premier advanced cyber weapon crafted for remote infiltration and semi-autonomous operation. Renowned German expert Ralph Lagner described Stuxnet as a military cyber missile responsible for launching a comprehensive cyber assault against the Iranian nuclear energy program, resulting in a significant 23% reduction in enrichment between mid-2009 and 2010.[62] The Tallinn Manual reflects the principles of customary international law based on a meticulous review of Article 2(4) of the UN Charter. The analysis of the use of armed force in response to the Stuxnet attack shows that the attack could be classified as a use of force under Article 2(4). This is primarily due to the substantial harm it inflicted, comparable to the damage caused by armed force in a physical context.[63] To better understand the situation, it is important to compare how things were before the Stuxnet virus emerged. At that time, cyber attacks were mostly focused on gathering information or disrupting services. Only a few instances of cyber attacks caused physical damage to infrastructure. This cyber attack marked a pivotal moment in the realm of cyber warfare. It unequivocally demonstrated that cyber weapons can cause destruction and disruption comparable to conventional or non-conventional weapons.

This attack's severity and widespread impact underscores the urgent need for heightened cybersecurity measures.

Section II : Approaches and standards are employed to identify the characteristics of cyber power. In this section, we will delve into the intricate and contentious issues surrounding the identification and characterization of cyberattacks in legal and political research. Specifically, we will consider the threshold at which digital directives can be classified as cyber-attacks. Throughout the years, numerous methodologies and standards have emerged to define the essence of cyber power, with some focusing on objectives, tools, and repercussions. In contrast, others adhere to criteria established by Professor Michael Schmitt and the Tallinn Manual. We will thoroughly explore these concepts in the parts that follow:

First: Approaches adopted in the description of cyber power

The majority of jurists strive to define the current legal framework for the use of force. They focus on a legal argument on whether cyber attacks should be considered a force, as outlined in paragraph (4) of Article (2) of the Charter.[64] This argument relies on three main approaches to describing the nature of cyber power: the goal-based approach, the tool-based approach, and the results-based approach (effects). We will discuss successively:

A. Objective-based approach: This particular approach focuses on the objective of a cyber attack. It can be described as follows: "A cyber operation is deemed to have crossed the threshold of the use of armed force when it is aimed at targeting national critical infrastructure, regardless of the nature of the operation and its impact on that structure.[65] This approach was developed for self-defence. Proponents believe that the current legal framework for using force provides adequate protection to targeted states. They argue that it enables attacked states to resort to force as a self-help measure when national critical infrastructure is targeted.[66] In simpler terms, cyber attacks will be considered a use of armed force based on their objective, regardless of how severe they are. For example, if a cyber attack targets the electronic system of dams or power plants, leading to water supply shutdowns or power outages in a country, it would be seen as using armed force. We believe that this approach should consider the nature of the targeted national infrastructure when determining the severity of a cyber attack, including its scope and effects.

B. Tool-based approach : This approach emphasizes the critical importance of the specific means utilized in "armed attack" and "armed force." It delves into the nature of the weapons employed, distinguishing them from other methods, such as economic and political coercion.[67] Some critics argue that this approach places excessive emphasis on physical properties to describe warfare, disregarding the significance of digital codes used in cyber attacks. Consequently, they maintain that cyber-attacks should not be classified as using force under

Article 2, paragraph 4, of the UN Charter, even when they result in tangible harm.[68] The legal field faces increasing challenges, particularly in defining the characteristics of means and combat methods. While the traditional approach based on the characteristics of kinetic energy weapons has been practical in the past, the rise of new technologies, especially digital ones, has made this approach less relevant. The challenge lies in classifying digital programs as weapons due to their dual or multi-purpose uses, undermining traditional methods of weapon classification. The concept of weapons in international law should not be narrowly interpreted. In 1996, the International Court of Justice, in its advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, explicitly affirmed that the provisions of Article 2(4), Article 42, and 51 of the Charter of the United Nations do not refer to specific weapons to which the concept of the use of force applies.[69] Some argue that weapons are primarily a means of confronting the enemy's human and material forces and are defined by their impact on the situation, not just by their nature.[70] The concept of means and methods of warfare is vital to understand. According to Maurice Aubert, means of warfare are the actual weapons, while methods of warfare refer to how they are used[71]". This definition applies to cyber attacks as well. A cyber attack is considered warfare if it directly or indirectly causes death, injury, destruction, or total or partial disruption. Furthermore, it is regarded as a method of warfare if it is

employed as part of a military plan to disable or destroy electronic air defence systems during or even before the commencement of hostile operations. Based on recent events, it is clear that the Russian forces disrupted the Ukrainian defence and air communication systems in 2022 before using conventional armed forces to invade Ukraine on February 24 of the same year. This highlights the significance of cyber attacks as a method of combat that can provide a direct military advantage in implementing a military plan, preceding the direct use of conventional armed forces such as missiles.[72] Several dual-use technologies, like lasers, which have various peaceful applications, such as in medicine, can also serve as weapons to inflict physical harm. As new warfare technologies emerge, it is crucial for states to acknowledge that cyber-attacks should be categorized as military weapons, akin to biological or chemical weapons.[73] Cyber attacks, though unconventional, can cause damage comparable to traditional kinetic weapons and should be considered a legitimate form of warfare.[74]

c. Results-based approach or (impacts): This approach is widely supported by most international legal scholars who have studied the subject in detail.[75] It is an approach based on analyzing consequences, namely physical destruction or loss of life. According to this approach, a cyber attack that results in physical destruction or loss of life should be considered a use of force. In essence, a cyber attack that causes or is likely to cause harmful consequences comparable to those caused by

conventional kinetic weapons should be classified as a use of force. The concept of "harm" should be clearly defined. It could include the destruction or malfunction of a device. In addition, there is an ongoing debate about including non-material consequences. For example, targeting intangible cultural property, such as a website that preserves cultural heritage, such as sacred verses or songs, raises questions about the criminal consequences of its destruction that amount to the use of armed force. Finding an answer to this question brings us back to the fundamental principle of unnecessary pain. Thus, even if a cyber attack that results in massive suffering is non-material, it should be considered a use of armed force.[76] In assessing a cyber attack, the classification as an armed attack is determined by the overall severity of its effects.[77] This approach offers a balanced perspective, bridging the gap between tool- and target-based methods, and enjoys widespread acceptance. Despite the crucial importance of the results-based approach, Marco Rossini advocates integrating the three approaches in analysis and evaluation. He proposes enhancing this approach by incorporating elements of the goal- and tool-based approaches.[78] According to Rossini, this combined approach will provide the most comprehensive framework for analyzing whether cyberattacks fall within the scope of the United Nations Charter and fulfil the requirements of Article 2, paragraph 4.[79] It is essential to assess each cyber operation on a case-by-case basis due to its unique nature and impacts in terms of intensity and type. Reinforcing this viewpoint, the ICJ has underscored that the "scope and effects" must be considered when determining if certain

acts of armed violence constitute an "armed attack.[80] As outlined in the Tallinn Manual, a cyberattack qualifies as the use of force when its scale and impact are comparable to non-cyberattacks that meet the threshold for the use of force.[81] The United States follows a results-based approach, supported by a 1999 Pentagon study, which emphasized the international community's focus on the consequences rather than the method of a cyber network."[82] his position was reiterated by State Department Legal Advisor Harold Koh in his 2012 address to the Interagency Legal Conference (USCYBERCOM), highlighting that if a cyber-attack's physical repercussions mirror those of a bomb or missile, it should, under specific conditions, be considered a use of force within the scope of Article 2(4) of the UN Charter and customary international law".[83] According to the latest study released in 2023, specific international legal instruments, while not yet legally binding or explicitly addressing issues such as cyberattacks, are still helpful for dealing with or adjusting to cyberattacks, especially when there are no relevant treaty provisions.[84] This can be seen as preliminary steps towards creating customary rules regarding the use of cyber force.

Second: Schmitt criteria and Tallinn Manual to Determine the Scope and Effects of Cyber Attacks In the Tallinn Manual, Michael Schmitt and a team of international experts have defined eight legal and policy criteria to assess cyber attacks with destructive consequences effectively. These criteria allow for comparing non-material cyber

damage to the physical impact of traditional kinetic energy attacks.[85] The criteria are:

A- Severity of damage: This criterion focuses on assessing the extent of damage caused by a cyber attack, including destruction, disability, and the scale of injury leading to death. The far-reaching consequences, such as material damage to individuals or property, elevate the cyber attack to the level of the use of force. Such consequences must impact any state's supreme national interests, further enhancing this criterion's significance. Additionally, contextual circumstances will amplify the evaluation of the cyber attack. The scope, duration, and severity of the damage, with the latter being the most crucial element, determine the classification of the cyber attack as the use of armed force in its legal sense.[86] B- Immediacy: This refers to measuring the time elapsed between a cyber attack and the resulting damage. Cyber attacks that have an immediate impact are more likely to be seen as the use of force compared to those that take weeks or months to have an effect. In simpler terms, when the consequences of an attack show up sooner, states are less likely to work towards a peaceful resolution of the conflict or take steps to stop the adverse effects from happening again and spreading. Therefore, states are more worried about the damage that happens simultaneously as the attack rather than the damage that appears later or gradually builds up in the future.[87] C. Directness : refers to the direct link between the use of armed force and its negative

consequences, as opposed to other forms of coercion such as political or economic means.[88] But, the less severe the initial act and its consequences, the less likely it is for the state to be held responsible for violating the prohibition on using armed force. This criterion assesses the factor of directness and causation. In armed actions, cause and effect are closely related; for instance, an "explosion" directly harms people or objects. Applying this to cyberattacks, the ones in which cause and effect are clear and directly connected are more likely to be categorized as using force compared to those in which cause and effect are not directly connected.[89] D- Invasion: In conventional military attacks, the forces of one state move to penetrate the defences of another state's forces and then take control of its territory. While this does not usually happen in the case of economic or political coercion, it cannot be denied that it is a use of force but cannot be considered armed. However, in the cyber context, this criterion analyzes the level of cyber aggression against violating the targeted state's sovereignty. The more the cyber attack penetrates the effectiveness of the state's sovereignty and control over its territory, the more it becomes a cyber invasion. It is a widespread espionage tool in the modern era. Still, it does not constitute a use of force or an armed attack, according to the rules of current international law, as long as the target remains within the scope of espionage and without tangible physical control.[90] C. Ability to determine effects: This refers to the ease and certainty in

assessing the consequences of armed force compared to other forms of coercion.[91] Essentially, this means attack damage assessment. In cyber operations, the consequences may be less clear and more challenging to measure. The more measurable the set of consequences is, the more indicative it is of the scale of interests affected, such as the number of deaths, destroyed buildings, and compromised sites.[92] D. Hypothetical legality :The inherent nature of international law prohibits certain conduct, assuming the opposite to be true. For instance, in an ongoing armed conflict, international law does not prohibit the use of rumours, psychological warfare, or espionage. These activities are presumed legitimate if they are used in a cyber context.[93] E. State responsibility: This criterion assesses the state's relationship to cyber attacks. The State can engage in these attacks with complete control or with non-state entities demonstrating effective control. According to the 2001 Draft on State Responsibility for Wrongful Acts and Articles 4 and 8, the stronger the relationship between the State and cyber attacks, the more likely they are to be classified as using armed force.[94] F. Military character: This criterion was added by the International Group of Experts when drafting the Tallinn Guide (2.0)According to this criterion, the more a cyber attack is related to operations in general and hostile operations in particular, the greater the likelihood of characterization as the use of force, which is confirmed by the Charter of the United Nations when it deals specifically with military actions, as it stipulates in

its preamble that: "Armed force shall not be used except in the common interest",[95] while Article (44) of UN charter uses the term "force" without the condition of "armed".[96] This is a situation that clearly indicates the use of military force. Moreover, it is a traditional notion that the use of force would imply force used by the army or any other armed forces, and the military nature of the cyberinfrastructure from which the cyber attack is directed is considered under the Charter in the characterization of attack contexts as the use of armed force.[97] After considering the abovementioned criteria, we must ask: Are they enough to describe armed attacks within the concept of using armed force? In response, we can say that the above criteria are not sufficient to describe cyber attacks as falling under the concept of the use of armed force. This is because classifying a cyber attack as armed depends on various circumstances. States may consider additional factors, such as the prevailing political environment, the level of the attack indicating potential future military force usage, the identity of the attacker, any history of cyber attacks by the attacker, and the nature of the target.

It is important to note that the "use of force" and "armed attack" serve different normative purposes, especially when cyber attacks are considered armed attacks. The "use of force" criteria determine whether a State has violated Article 2, paragraph 4 of the Charter of the United Nations and the related prohibition of customary

international law. This differentiation holds legal significance because using force alone does not justify a response using force. According to the International Group of Experts, a State facing the use of force that does not amount to an "armed attack" must resort to other measures if it wishes to respond lawfully, such as countermeasures or measures in line with the principle of military necessity.[98]

Conclusion

In an age of digital warfare, where lines of code can become tools of conflict, reconciling cyberattacks with the UN Charter's prohibition on using force takes on unprecedented urgency. The transition from traditional battlefields to the virtual world requires a nuanced understanding of what constitutes an "armed attack" and how we can effectively apply ancient legal principles to new forms of aggression. As we navigate this complex intersection of technology and international law, it is clear that the UN Charter's enduring commitment to peace and security must evolve alongside the cyber domain. The Tallinn Manual provides a critical framework yet remains a work in progress, reflecting the ongoing struggle to define and regulate cyber hostilities. Our exploration reveals that the essence of the Charter's prohibition on force lies not just in the manner of aggression but in the harm inflicted. As cyberattacks become increasingly sophisticated, so must our legal

definitions and responses. The challenge is to strike a balance that protects international peace while recognizing the distinctive nature of cyber operations. Moving forward, we must strengthen international cooperation and develop adaptable legal norms that address the unique characteristics of cyber conflict. This development will require not only legal innovation but also a global commitment to understanding and mitigating the risks of cyber warfare. By bridging the gap between law and conflict, we can hope to preserve the spirit of the UN Charter while effectively addressing the realities of modern threats. We conclude that we should not interpret the prohibition on using force under Article 2(4) of the UN Charter in the same way as the right to self-defence under Article 51. The traditional understanding of kinetic force should be reconsidered, as the broad and immediate impact of using non-kinetic methods such as cyberattacks or armed force can be considered an armed attack under the UN Charter's definition of the use of force. It is imperative that we remain steadfast in our commitment to peace and security as methods of force evolve, particularly in the face of digital attacks. To truly address the future of conflict in the digital age, we must embrace solutions that bridge the legal gap and effectively address the challenges posed by digital technology compared to the rigidity of legal rules. In an era where the

digital realm is increasingly marred by aggressive cyber assaults, harmonizing the UN Charter's prohibition on using force with the complexities of these attacks proves to be a formidable challenge. To navigate this tangled web, we propose a collaborative endeavor led by the United Nations to forge a groundbreaking international pact. This agreement would define a binding code of conduct for cyber activities rooted firmly in the principles of the UN Charter. Our approach hinges on three pivotal elements: First, the UN Charter's cornerstone—Article 2, Paragraph 4—forbids using armed force alongside Article 51, which permits exceptions for self-defence. Second, the inclusion of Article 8 bis from the International Criminal Court's Statute addresses the crime of aggression. Finally, the creation of a dedicated international agreement specifically targeting aggressive cyber conduct.

By weaving these elements together, we aim to craft a clear and unified global stance against the murky threats of digital aggression, ensuring a robust and coherent response to the evolving challenges of cyber conflict.

[1] Prescott, Jody M. Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States? International Conference on Cyber Conflict (CYCON 2012). IEEE, 2012, p. 253.

[2] Melzer, Nils. Cyberwarfare and international law. United Nations Institute for Disarmament Research, 2011. p. 7-8; also see Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, 1998-1999, Vol. 37, p. 916.

[3] United Nations General Assembly, document (A/68/98) of 24 June 2013, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 19, p. 9.

[4] Marco Roscini, Cyber Operations and the Use of Force in International Law, OUP Oxford, UK, 2014, pp. 44-45.

[5] ICJ. Report 1996 Legality of the Threat or Use of Nuclear Weapons, International Court of Justice July 8, 1996 ,General List No. 95, para. 47.

[6] ICJ, REPORTS OF JUDGMENTS, ADVISORY OPINIONS AND ORDERS CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA) JURISDICTION OF THE COURT AND ADMISSIBILITY OF THE APPLICATION JUDGMENT OF 26 NOVEMBER 1984, para. 91.

[7] Schmitt MN In: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press; 2017. Comment (1) on Rule (69).

[8] Marco Roscini, Gravity in The Statute of The International Criminal Court and Cyber Conduct That Constitutes, Instigates or Facilitates International Crimes, Criminal Law Forum, Vol. 30 (3), 2019,p.249.

[9] François Delerue, Cyber Operations and International Law, Cambridge, UK, 2020, p. 288.

[10] Ahmed Aubais Al-Fatlawi, "Cyber Attacks: An Analytical Legal Study on the Challenges of its Contemporary Organization", Zain Law and Literary Library, Beirut, Lebanon, 2018., pp. 11-12.

[11] Michael N Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, op.cit, p. 890.

[12] DoD Dictionary of Military and Associated Terms, The Joint Staff, Office of the Chairman of the Joint Chiefs of Staff, Washington DC, 2015, p. 55.

[13] Schmitt MN In: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, op. cit. Rule (92).

[14] DOD Dictionary of Military and Associated Terms, op.cit, p. 55.

[15] Ibid

[16] Jonathan A. Ophardt, Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield, Duke Law & Technology Review, 2010, Vol. 9, No. 3. para. 7.

[17] Ibid.

[18] Ibid

[19] Richard A. Clarke and Robert K. Knake, Cyber War the Next Threat to National Security and What to Do About It, HarperCollins, U.S.A, 2010, p.10.

[20] Jeffrey Carr, Inside Cyber Warfare, O'Reilly Media, U.S.A, 2nd ed, 2011, p. 2.

[21] James A. Green, Cyber Warfare A multidisciplinary analysis, Routledge, London, UK, 2015, p. 2.

[22] James A. Green, op. cit, p 3.

[23] Katie Terrell Hanna & Kevin Ferguson & Linda Rosencrance Definition Cyber warfare, Tech Target network, 21 May 2021. Available at: https://searchsecurity.techtarget.com/definition/cyberwarfare

[24] Cornish, Paul, On cyber warfare. Chatham House, London, 2010. p. 1.

[25] Robinson, Michael, Kevin Jones, and Helge Janicke. Cyber warfare: Issues and challenges. Computers & Security, 2015, Vol. 49, p. 73.

[26] Bell, Cameron H, Cyber Warfare and International Law: The Need for Clarity. Towson University Journal of International Affairs, 2018, vol. 51. No. 2, p. 26.

[27] Ibid,pp.26-27.

[28] Jonathan A. Ophardt, Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield, Duke Law & Technology Review, 2010, Vol. 9, No. 3. para. 8.

[29] Ibid, para. 9.

[30] James L. Regens & Charles B. Vandepeer Piercing the Veil of Darkness? Deception and Intelligence in Warfare, JOURNAL OF MILITARY AND STRATEGIC STUDIES, VOLUME 22, ISSUE 3,2023, pp.21-22.

[31] Solce, Natasha. The battlefield of cyberspace: The inevitable new military branch-the cyber force. Albany Law Journal of Science & Technology. 2008, Vol, 18, pp. 293-301

[32] Marco Roscini, Cyber Operations and the Use of Force in International Law, op.cit, pp. 10-11.

[33] Hathaway, Oona A., et al. The law of cyber-attack. California Law Review, 2012. vol. 100, No. 4, pp. 833-841.

[34] Mona al-Ashqar Jabbour, "Cyber is the Obsession of the Age", League of Arabic States, Arab Center for Legal and Judicial Research, Beirut, 2016, p. 28.

[35] Jonathan A. Ophardt, op.cit. para. 10.

[36] Herzog, Stephen. Revisiting the Estonian cyber-attacks: Digital threats and multinational responses. Journal of Strategic Security,2011, vol.4, No. 2. pp. 51-52.

[37] Shackelford, Scott J. From nuclear war to net war: analogizing cyber-attacks in international law. Berkeley Journal of International Law, 2009, Vol. 27 Issue. 1.p. 206.

[38] Ibid.p, 207.

[39] Ibid. p, 208.

[40] Ibid, p. 207.

[41] James A. Green, Cyber Warfare A multidisciplinary analysis, op.cit, p. 18.

[42] Christopher Whyte, Brian Mazanec, Understanding cyber warfare: politics, policy and strategy, Routledge, U.S.A, New York, 2019, pp. 222-223.

[43] Christopher Whyte, op. cit, p. 254.

[44] Ibid, p. 109.

[45] James A. Green, Cyber Warfare A multidisciplinary analysis, op.cit, p. 18.

[46] Ibid, p. 18.

[47] Ibid, p. 19.

[48] Ibid.

[49] Christopher Whyte, Brian Mazanec, op.cit, p.109.

[50] James A. Green, Cyber Warfare A multidisciplinary analysis, op.cit, p. 19.

[51] Ibid, p. 19.

[52] Ibid, p. 20.

[53] Gross, Michael Joseph. A declaration of cyber-war. Vanity Fair Journal, 2011, vol. 53, no.4. p. 7.

[54] Ibid.

[55] Thomas Rid, Cyber War Will Not Take Place, Oxford University Press, UK, 2013, pp. 43 - 72.

[56] Ibid, pp. 72.

[57] Gross, Michael Joseph. A declaration of cyber-war. Vanity Fair Journal, 2011, vol. 53, no.4. p. 13.

[58] Ibid, p. 32.

[59] Ibid, p. 43.

[60] Ibid, p. 44.

[61] Ibid, p. 45.

[62] James P. Farwell & Rafal Rohozinski Stuxnet and the Future of Cyber War, Survival journal, the International Institute for Strategic Studies, 2011, vol, 53, No. 1, pp. 123- 129.

[63]Kinetic is a Latin infinitive term The word Kinetic comes from the Greek word kinētikos, which means "movement", which in turn follows the verb kinein which means "to move, and relates to the movements of physical bodies and the forces and energy associated with them, see: *Merriam-Webster.com Dictionary*, Merriam-Webster, https://www.merriam-webster.com/dictionary/kinetic. Last accessed 17 Aug. 2024

[64] Marco Roscini, Cyber Operations and the Use of Force in International Law, op.cit, p. 46. ; & François Delerue, Cyber Operations and International Law", Cambridge University Press, UK, 2020, p. 288.

[65] Chaumette, AL. International Criminal Responsibility of Individuals in Case of Cyberattacks. International Criminal Law Review, 2018, Vol. 18, No. 1, p. 8.

[66] François Delerue, op.cit, p. 288.

[67] Marco Roscini, Cyber Operations and the Use of Force in International Law, op.cit, p. 46

[68] Ibid, p. 47.

[69] 1CJ. Report 1996 Legality of the Threat or use of Nuclear Weapons, op.cit, para. 39.

[70] Chaumette AL, op.cit, p. 7.

[71] Murice Aubert, The ICRC and the problem of excessively injurious or indiscriminate weapons, Extract print from IRRC, no 279, Nov-Dec, 1990, p.483.footnote.18.

[72] Cyberattacks rose at the beginning of 2022, for example, on January January 13, *Microsoft* reported that malware targeting the Ukrainian government and several non-profit organizations and IT organizations was

detected, and the next day, 70 government websites ended up being disrupted , including the website of the Cabinet of Ministers and the Ministries of Defense, Foreign Affairs February, Education and Science. Several countries accused Russia of launching the attack to cause panic and confusion among Ukrainians, while the same sites, including the website of the Council of Ministers and several ministries, were repeatedly targeted again on February 23 as well as the launch of *the Hermetic Wiper* malware against 100 financial, IT and aviation institutions. For more information see:
Jakub Przetacznik with Simona Tarpova, Russia's war on Ukraine: Timeline of cyber-attacks, European Parliamentary Research Service,Members' Research Service, PE 733.549, June 2022.p.3.

[73] Michael N Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, op.cit, p. 914; Chaumette AL, op.cit, p. 7.

[74] Dinstein, Yoram Cyber war and international law: concluding remarks at the 2012 Naval war college international law conference. International Law Studies, 2013, vol. 89, No.1.p. 280.

[75] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, Cambridge University Press, UK, 2012, p. 74.

[76] Fatlawi, A.A. Protecting Cultural Heritage in Times of War: A Study of the Gravity of Protection Rules vs the Weight of Violations. In: Mastandrea Bonaviri, G., Sadowski, M.M. (eds) Heritage in War and Peace. Law and Visual Jurisprudence, vol 12. Springer, Cham (2024), p. 243.

[77] Marco Roscini, Cyber Operations and the Use of Force in International Law, op.cit, p. 47.; Silver, Daniel B. op.cit, p. 89.; Hathaway, Oona A, op.cit,p. 847. ; Chaumette AL, op.cit, p. 8.

[78] Ibid, p. 50.

[79] François Delerue, Cyber Operations and International Law, op.cit, p. 290.

[80] ICJ, REPORTS OF JUDGMENTS, ADVISORY OPINIONS AND ORDERS CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA, op. cit, para. 91.

[81] Schmitt MN. In: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, op.cit, Rule (69).

[82] U.S. Department of Defense, Assessment of International Legal Issues in Information Operations, May 1999, p. 18, available at: https://fas.org/irp/eprint/io-legal.pdf Last visited 31-Aug-2024

[83] Harold Koh, "International Law in Cyberspace," Speech at the Inter-Agency Legal Conference (USCYBERCOM), September 18, 2012, referred to as Koh in Cyberspace, available at: https://harvardilj.org/2012/12/online_54_koh/. Last visit 18-Aug-2024

[84] Gabriella Blum, The Shadow of Success: How International Criminal Law Has Come to Shape the Battlefield, the Stockton Center for International Law,Vol.100,2023,pp.140-141.

[85] Michael N Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, op.cit, p. 914. ; also, Schmitt MN In: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,op.cit, Comment (9) on Rule (69).

[86] Schmitt MN In: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,op.cit, Comment (9) on Rule (69).

[87] Ibid, Comment (9) on Rule (69)

[88] Silver, Daniel B. op. cit, p.89.

[89] Schmitt MN In: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, op.cit, Comment (9) on Rule (69).

[90] Ibid, Comment (9) on Rule (69). Comment (9) on Rule (69).

[91] Silver, Daniel B, Computer network attack as a use of force under Article 2 (4) of the United Nations Charter." International Law Studies,, vol. 76. No.1, 2002, p. 90.

[92] Schmitt MN In: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, op.cit, Comment (9) on Rule (69).

[93] Ibid, Comment (9) on Rule (69). also see Schmitt, Michael N. Cyber operations in international law: The use of force, collective security, self-defence, and armed conflicts. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy, 2010, Vol. 151, pp. 155-156; also see: Jeffrey Carr, op.cit, p. 61.

[94] Schmitt MN In: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, op. cit, Comment (9) on Rule (69). ; also see, Schmitt, Michael N. Ibid, pp. 155-156.

[95] (Preamble) Charter of the United Nations.

[96] Ibid. Article (44).

[97] Schmitt MN In: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, op.ct, Comment (9) on Rule (69).; also see Kriangsak Kittichaisaree, Public International Law of Cyberspace, Springer, Switzerland, 2017, p. 165.

[98] Tallinn Manual 2.0, op.cit, Comment (10/11) on Rule (69).

References :

1. Ahmed Aubais Al-Fatlawi, "Cyber Attacks: An Analytical Legal Study on the Challenges of its Contemporary Organization", Zain Law and Literary Library, Beirut, Lebanon, 2018.

2. Bell, Cameron H, Cyber Warfare and International Law: The Need for Clarity, Towson University Journal of International Affairs, vol. 51. No. 2. 2018.

3. Chaumette, AL. International Criminal Responsibility of Individuals in Case of Cyberattacks. International Criminal Law Review, Vol. 18, No. 1, 2018.

4. Christopher Whyte, Brian Mazanec, Understanding cyber warfare: politics, policy and strategy, Routledge, U.S.A, New York, 2019.

5. Cornish, Paul, On cyber warfare. Chatham House, London, 2010.

6. Dinstein, Yoram. Cyber war and international law: concluding remarks at the 2012 Naval War College International Law Conference. International Law Studies, vol. 89, No.1, 2013.

7. DoD Dictionary of Military and Associated Terms, The Joint Staff, Office of the Chairman of the Joint Chiefs of Staff, Washington DC, 2015.

8. Fatlawi, A.A. Protecting Cultural Heritage in Times of War: A Study of the Gravity of Protection Rules vs the Weight of Violations. In: Mastandrea Bonaviri, G., Sadowski, M.M. (eds) Heritage in War and Peace. Law and Visual Jurisprudence, vol 12. Springer, Cham,2024.

9. François Delerue, Cyber Operations and International Law", Cambridge University Press, UK, 2020.

10. François Delerue, Cyber Operations and International Law, Cambridge, UK, 2020.

11. Gabriella Blum, The Shadow of Success: How International Criminal Law Has Come to Shape the Battlefield, Stockton Center for International Law, Vol. 100, 2023.

12. Gross, Michael Joseph. A declaration of cyber-war. Vanity Fair Journal, vol. 53, no.4,2011.

13. Gross, Michael Joseph. A declaration of cyber-war. Vanity Fair Journal, vol. 53, no.4, 2011.

14. Harold Koh, "International Law in Cyberspace," Speech at the Inter-Agency Legal Conference (USCYBERCOM), September 18, 2012, available at: https://harvardilj.org/2012/12/online_54_koh/

15. Hathaway, Oona A., et al. The law of cyber-attack. California Law Review, vol. 100, No. 4,2012.

16. Heather Harrison Dinniss, Cyber Warfare and the Laws of War, Cambridge University Press, UK, 2012.

17. Herzog, Stephen. Revisiting the Estonian cyber-attacks: Digital threats and multinational responses. Journal of Strategic Security, vol.4, No. 2, ,2011.

18. ICJ, REPORTS OF JUDGMENTS, ADVISORY OPINIONS AND ORDERS CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA) JURISDICTION OF THE COURT AND ADMISSIBILITY OF THE APPLICATION JUDGMENT OF 26 NOVEMBER 1984.

19. ICJ. Report 1996 Legality of the Threat or Use of Nuclear Weapons, International Court of Justice, General List No. 95, July 8, 1996.

20. Jakub Przetacznik with Simona Tarpova, Russia's war on Ukraine: Timeline of cyber-attacks, European Parliamentary Research Service, Members' Research Service, PE 733.549, June 2022.

21. James A. Green, Cyber Warfare A multidisciplinary analysis, Routledge, London, UK, 2015.

22. James L. Regens & Charles B. Vandepeer Piercing the Veil of Darkness? Deception and Intelligence in Warfare, JOURNAL OF MILITARY AND STRATEGIC STUDIES, VOLUME 22, ISSUE 3,2023.

23. James P. Farwell & Rafal Rohozinski Stuxnet and the Future of Cyber War, Survival journal, the International Institute for Strategic Studies, vol, 53, No. 1, 2011.

24. Jeffrey Carr, Inside Cyber Warfare, O'Reilly Media, U.S.A, 2nd ed, 2011, p. 2.

25. Jonathan A. Ophardt, Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield, Duke Law & Technology Review, Vol. 9, No. 3,2010.

26. Jonathan A. Ophardt, Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield, Duke Law & Technology Review, Vol. 9, No. 3,2010.

27. Katie Terrell Hanna & Kevin Ferguson & Linda Rosencrance Definition Cyber warfare, Tech Target network, 21 May 2021. Available at: https://searchsecurity.techtarget.com/definition/cyberwarfare

28. Kriangsak Kittichaisaree, Public International Law of Cyberspace, Springer, Switzerland, 2017.

29. Marco Roscini, Cyber Operations and the Use of Force in International Law, OUP Oxford, UK, 2014.

30. Marco Roscini, Gravity in The Statute of The International Criminal Court and Cyber Conduct That Constitutes, Instigates or Facilitates International Crimes, Criminal Law Forum, Vol. 30 (3), 2019.

31. Melzer, N.s. Cyberwarfare and international law. United Nations Institute for Disarmament Research, 2011.

32. Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/kinetic

33. Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, 1998-1999, Vol. 37.

34. Mona al-Ashqar Jabbour, "Cyber is the Obsession of the Age", League of Arabic States, Arab Center for Legal and Judicial Research, Beirut, 2016.

35. Murice Aubert, The ICRC and the problem of excessively injurious or indiscriminate weapons, Extract print from IRRC, no 279, Nov-Dec, 1990.

36. Prescott, Jody M. Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States? International Conference on Cyber Conflict (CYCON 2012). IEEE, 2012

37. Richard A. Clarke and Robert K. Knake, Cyber War The Next Threat to National Security and What to Do About It, HarperCollins, U.S.A, 2010.

38. Robinson, Michael, Kevin Jones, and Helge Janicke. Cyber warfare: Issues and challenges. Computers & Security, Vol. 49. 2015.

39. Schmitt MN In: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.

40. Schmitt, Michael N. Cyber operations in international law: The use of force, collective security, self-defence, and armed conflicts. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy, 2010, Vol. 151.

41. Shackelford, Scott J. From nuclear war to net war: analogizing cyber-attacks in international law. Berkeley Journal of International Law, Vol. 27 Issue. 1, 2009.

42. Silver, Daniel B, Computer network attack as a use of force under Article 2 (4) of the United Nations Charter." International Law Studies, vol. 76. No.1, 2002.

43. Silver, Daniel B. Computer network attack as a use of force under Article 2(4) of the United Nations Charter. International Law Studies, vol. 76, no. 1, 2002.

44. Solce, Natasha. The battlefield of cyberspace: The inevitable new military branch–the cyber force. Albany Law Journal of Science & Technology, Vol. 18, 2008.

45. Thomas Rid, Cyber War Will Not Take Place, Oxford University Press, UK, 2013.

46. U.S. Department of Defense, Assessment of International Legal Issues in Information Operations, May 1999, available at: https://fas.org/irp/eprint/io-legal.pdf Last visited 31-Aug-2024

47. United Nations General Assembly, document (A / 68/98) of 24 June 2013, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.