FUTURITY OF SOCIAL SCIENCE

DOI: https://doi.org/10.57125/FS.2023.03.20.03

How to cite: Svitlak, I. (2023). Cyber Military Threat and International Law: Assessing the Response to Cyber Attacks in the Military Context. *Futurity of Social Science, 1*(1),. 35-50. https://doi.org/10.57125/FS.2023.03.20.03

Cyber Military Threat and International Law: Assessing the Response to Cyber Attacks in the Military Context

Iryna Svitlak

Doctor in Juridical Sciences, Associate Professor, Vinnytsia Education and Research Institute of Economics, West Ukrainian National University, Vinnytsia, Ukraine, https://orcid.org/0000-0002-4408-6868

Correspondence email: *SvitlakIryna@gmail.com.*

Received: December 2, 2022 | **Accepted:** February 11, 2023 | **Published:** March 20, 2023

Abstract: The purpose of the article is to analyse cyber-military threats through the prism of assessing the response to cyber-attacks in international law. To achieve this goal, the author used the scientific methods of analysis, synthesis, content analysis, and the dogmatic method. Using the proposed methodology, 51 professional studies were analysed, which allowed for an impartial approach to the assessment of the main issue. The results show that one of the key difficulties is identifying the parties to the conflict, as cyberattacks are not limited by state borders, and identifying their initiator can be difficult. The problem of determining the subject of responsibility, in particular in cases of actions of civilian personnel, makes the definition of the conflict as a military one more uncertain. Under the UN Charter, the use of force between states is limited, making it difficult to unify the rules of cyber warfare at the international level. The terms "cyberwar" and "cyberattacks" are applied to potentially dangerous operations in digital networks, but their definition and regulation remain open questions. All of this requires new approaches and international standards to effectively regulate and ensure security in cyberspace, in particular, given its unique aspects and impact on international relations. The Tallinn Book, which is an informal collection of expert opinions, examines issues such as the definition of cyberattacks, self-defence in cyberspace, and the application of the principle of non-use of force in the digital environment. This document may serve as a basis for a future international convention that will regulate legal relations in cyberspace at the international

level. The conclusions emphasise that without the political will of international actors, the solution to the problems of countering cyber warfare is hampered.

Keywords: Tallinn Book, international law, cyberwar, cyberconflict, digital environment.

Introduction

In today's information age, where technological progress and digital transformation intersect with geopolitical challenges, cybersecurity is becoming a critical issue. Cyber warfare is becoming not only a challenge to national security, but also a challenge to international stability and peace. Therefore, the development of cyber armed forces and the existence of cyber threats are now becoming key challenges to the national security and sovereignty of countries in the growing digital age (Pang & Li, 2020). According to Ayalew (2015), modern societies have become extremely dependent on information technology and digital systems. For the sake of efficiency and development, countries use and implement digital technologies, but this also creates vulnerabilities that can be exploited in attacks. In addition, it is worth considering that cyberattacks can affect not only information systems, but also critical infrastructure, energy networks, financial systems, and other strategically important objects (Crespo, 2018). This poses a threat to economic and social stability. Accordingly, an important and relevant area of research is to study the dynamics of response to cyberattacks in the context of international law, especially in their interaction with military aspects (Thomas 2023; Kalpokiene, 2016). Undoubtedly, as Pang & Li (2020) have shown, the use of cyberattacks differs from armed aggression, but some amendments to the Geneva Conventions recognise that in the event of a new type of weapon, there is a need to supplement existing conventions rather than write new international documents. At the same time, an important problem of the Russian-Ukrainian war is that the aggressive actions of the Kremlin regime have threatened the existence of the post-World War II world order. The current challenge to the collective security system is obvious - Russian aggression has shown a clear disregard for existing international law.

Therefore, delving into the subtle threads of legal regulation, analysing the role of international institutions and states in this context, there is a need to reveal in more detail how effective modern international law is in ensuring cybersecurity in the face of growing tensions in cyberspace.

Research Problem

Therefore, the analysis of recent scientific publications has shown that the study of the cyber-military threat and international law through the prism of assessing the response to cyber-attacks in the military context and the analysis of modern international conventions on countering cyber threats as acts of war remain unresolved.

The problem of the study is that the development of cyberspace and its use for military purposes exceeds the traditional framework of international law. International legal instruments and norms were created mainly with traditional forms of conflict in mind, while cyber warfare threats require new approaches and recognition of the uniqueness of this type of conflict. One of the key challenges is that cyber-attacks can take a variety of forms and targets, sometimes unravelling traditional distinctions between civilian and military objectives. Consideration needs to be given to how international law can adapt to this new reality and how to respond effectively to such challenges while ensuring an adequate level of protection and accountability. An additional complication is the anonymity and difficulty of attribution of cyberattacks, which makes it difficult to identify perpetrators and enforce international accountability. In addition, the absence of generally accepted standards

in this area may create a legal vacuum, which can lead to ineffective measures to counter cyber aggressions. These aspects determine the importance and relevance of this study.

Research Focus

By analysing the use of cyberattacks in the context of international law, the article emphasises the interconnectedness of the current legal framework for interaction with military events in cyberspace. By examining precedents and responses to various cyberattacks, the article seeks to determine the extent to which these responses comply with international norms and rules. Particular attention will be paid to the role of international institutions such as the UN and the European Union in shaping and implementing strategies to counter cyberwarfare threats. In combination with the study of the Ukrainian experience, this will allow for the development of certain established models of legal response to cybersecurity challenges in the future. When analysing the current state of legislation and proposing possible directions for its further development, it is also important to pay attention to determining the effectiveness and modernity of legal mechanisms in ensuring cybersecurity in the context of the constant evolution of cyber threats and cyber weapons, and possible unstable development of the international political situation in Ukraine and the world.

Research Aim and Research Questions

The purpose of the article is to study the cyber-military threat and international law through the prism of assessing the response to cyber-attacks in the military context. The realisation of this goal requires finding answers to the following topical issues:

1. Consideration of international conventions on countering cyber threats as acts of war.

2. Formulation of recommendations for new legal documents that would establish responsibility for aggression in the cyber environment (the "Tallinn Book").

Literature Review

Researchers point to various aspects of the legal regulation of Internet crime and cyberwarfare, reflecting different perspectives and highlighting key trends in this area. Alnakeep (2022) highlighted the connection between Internet crimes and their legal regulation. The author explores topical issues related to the development of technology and the emergence of new forms of crime in virtual space. Maskun and Rum (2021) investigated cyber warfare as a variable method of warfare and its impact on national security. Valuch et al. (2017) also studied cyberattacks, information attacks, and postmodern warfare, examined the evolution of military activities in cyberspace and its impact on international law. Thomas (2023) analysed cybercrime and countermeasures to counter it, considered current issues related to cybersecurity, and offered recommendations for its prevention. Based on these studies, it is possible to trace the gradual evolution of ideas about the use of force in cyberspace, organisation and conduct of attacks, etc. This made it possible to identify certain fundamental provisions in understanding the theoretical basis on which the use of the legal system in overcoming the threat of cyber warfare is based.

Researchers have also considered the Tallinn Book as an important tool for regulating cyber warfare in the future. In particular, Boulos (2017) critically reviewed this publication in the context of its relation to the Jus Ad Bellum - the right to wage war. Nordström (2019) examined the regulation of cyber operations that do not reach the threshold set out in Article 2(4) of the UN Charter. The author analyses Rule 4 of the Tallinn Manual 2.0, which regulates this aspect of international law. Arnold (2020) discusses the contribution of the second edition of the book to the study of international law applicable to cyber operations - the author points out the key aspects and

innovations of this legal instrument. Dienelt (2022) examined the interplay between the laws of armed conflict, human rights, and international environmental law. His article proposes an expanded approach to the regulation of armed conflicts, taking into account the impact on human rights and the environment. Sweet (2014) and Tanodomdej (2019) also reviewed the Tallinn Book, which analyses international law applicable to cyber operations. The authors highlight the key aspects of the document and its significance for understanding the legal context of cyber warfare from a comparative perspective. Tsagourias (2013) outlined the peculiarities of the "use of force" in the Tallinn Book, analysing the use of force in the context of cyber operations and its compliance with international humanitarian law. At the same time, many critical aspects of the drafting and operation of the Tallinn Book will require further consideration, as the possible circumstances of the use of military force in cyberspace have changed significantly, and the Russian-Ukrainian war has demonstrated the reality of the use of cyberspace during hostilities.

Alsemairi (2022) examined the role of digital technologies in combating crimes related to human and arms trafficking via the Internet. The author analyses the effectiveness of modern technologies in combating cybercrime of this type. Dinniss (2015) focuses on the regulation of cyber warfare in accordance with the principles of jus in bello (the law of war). The author analyses the main aspects of legal regulation of cyber conflicts and their compliance with international standards. Simović et al. (2020) studied cyber warfare and international cyber law. The authors examine current trends and prospects in the development of cyber legislation and regulation of cyber warfare. Lancelot (2020) analysed the topic of cyber diplomacy, including cyber warfare and the rules of engagement. The author explores the challenges faced by modern cyber diplomacy and offers recommendations on the rules of engagement in cyber conflicts. Ayalew (2015) analysed the problem of cyber warfare and its reflection in international humanitarian law. The author examines the new challenges arising from the development of cyber-armed conflicts. Di Martino (2021) highlighted the role of fear and compassion in international relations, in particular in diplomacy, cyber engagement, and Australian foreign policy. Baradaran and Habibi (2017) studied cyber warfare from the perspective of international law, focusing on self-defence. The authors highlight important aspects of the legal regulation of cyber conflicts. Lucas (2017) analysed the international law applicable to cyber operations. The author discusses the ethical aspects of cyber warfare and recommendations for its regulation. Naidoo and Jacobs (2023) devoted their article to cyberwarfare and cyberterrorism, which pose a threat to critical infrastructure. The authors propose a framework model for analysing and understanding threats emanating from cyberspace. Trezza (2017) examined the negotiation of cyber warfare, focusing on the diplomatic aspects of resolving conflicts in cyberspace. Difficulties with anonymity in cyber warfare and the impact of this status on the prosecution of perpetrators in the context of international humanitarian law were traced by Buchan (2016). An important aspect is the analysis of those works that assert a certain theoretical platform for understanding the use of the legal framework in the field of cyber law. Thus, according to researchers, international law regulates the issue of protection against cyberattacks through a number of conventions, treaties, and other documents that regulate the behaviour of states in cyberspace. Several key aspects reflect how international law responds to cyber threats and cyber-attacks (see Table 1).

Table 1

Key legal aspects of the global community's response to cyber challenges

Aspect	Characteristics

Application of international law principles to cyberspace	The general principles of international law, such as sovereignty, non-intervention, non-aggression, and others, also apply in cyberspace. States must refrain from actions that violate these principles, even in cyberspace.
Declarations and conventions	A number of international instruments, such as the Convention on Cybercrime (the Budapest Principle), attempt to set standards for combating cybercrime. However, some of these instruments have not yet gained traction or gained widespread support.
The right to self-defence	Under international law, states have the right to self-defence in the event of an armed attack. If a cyberattack is considered an armed attack, a state may take self-defence measures, including cyber measures.
The process of identifying attacks	Determining when a cyber-attack is genuine is important. The process of identifying and attributing cyber-attacks can be an important step in determining how to respond.
International cooperation	Cooperation between international public institutions, states, and the private sector in the field of cybersecurity is becoming increasingly important. Measures to develop international standards and joint efforts to combat cyber threats are gaining attention.

Source: compiled by the authors based on Fleck (2013), Karska and Karski (2019), Mohamed Hassan and Mohamed Ali (2023).

Although there are still many challenges and uncertainties in this area, the development of international law reflects the need for joint action to ensure cybersecurity and accountability in cyberspace.

Research Methodology

General background

Analysing the cyber-military threat and international law in the context of assessing responses to cyber-attacks from a military perspective is important for several reasons. Firstly, it is important in the context of national security, as the development of cyber forces and the threat of cyber-attacks have become an essential element of the overall national security complex. On the other hand, an analysis of international law, which defines the rules and norms governing the behaviour of states in cyberspace, will help to understand the legal aspects of responding to cyber aggressions and develop appropriate strategies. Therefore, this study is qualitative and based on expert judgements, analysis of scientific literature, and the international legal framework.

Data collection

At the initial stage of the study, the content analysis method was used to process the scientific literature. In total, 51 items of professional publications in the main area of research were analysed. The selection of the necessary articles and monographs was carried out using Google Scholar search resources, with preference given to the most cited works and works published since 2013. This made it possible to avoid citing already somewhat anachronistic opinions, the relevance of which has decreased due to the rapid development of technology (and, accordingly, the legal interpretation of the use of force in cyberspace has undergone significant changes). To work with normative documents (UN charters and international conventions), the author also used the dogmatic method,

which made it possible to understand and describe the peculiarities of the legal interpretation of cyber military challenges in modern international law.

Data analysis

The article was written using the scientific methods of analysis and synthesis. In particular, the use of analysis made it possible to divide the main research problem into several smaller ones and thus analyse them more thoroughly. This made it possible to identify both problematic elements in the interpretation of the use of legal norms in cyber conflicts and to identify certain positions on which researchers have reached a certain agreement. This allows for further study of controversial issues and confirmation or refutation of the research findings of other scholars. The synthesis method was useful in writing the conclusions to the paper, as it was used to summarise the collected material and develop a broader concept in identifying further promising areas for research.

The work was carried out based on the principles of comprehensiveness and impartiality. For this reason, it was possible to avoid the dissemination of subjective opinions on the main issue of the scientific article.

Results

Using International Conventions to Counter Cyber Threats and Cyber-attacks in the Military Context

In terms of the application of international law, military operations in cyberspace (cyberwarfare) raise a number of complex issues. First of all, this includes the problem of identifying the parties to the conflict, since in the context of information confrontation, the means of influence are not defined by state borders and do not contain clear individual features, and their nationality can be determined only by certain indirect markers. Thus, identifying the initiator of the conflict becomes a problematic task, which, in the context of a cyberattack, can take a considerable amount of time (Kurebwa & Magumise, 2020). This also applies to the identification of the subject of responsibility (Orr, 2023). Cyber operations can be carried out by individuals who are not even aware of their role in the conflict. For example, civilian employees working for an internet company, which in turn performs tasks for an extraterritorial customer. Therefore, if it is impossible to identify the person, organisation, or country of the customer, it is difficult to define such activities as an operation of military conflict (Peresada, 2021). In addition, cyberattacks may undergo an incubation period when the threat does not manifest itself or does not contain certain critical dangers that cause devastating consequences. Thus, it becomes virtually impossible to determine the existence of a conflict at a given time. In addition, the identification of the parties to the conflict in real-time is also complicated by these factors.

According to the United Nations (UN) Charter, states are restricted from using force against other states, except when such use of force is under the authority of the UN Security Council or in situations of "individual or collective self-defense" against an "armed attack". Such exceptions do not contribute to a general, internationally accepted rule of cyber warfare (Richemond-Barak, 2023). The problems of different approaches to understanding forceful influence in information or cyber space, which were highlighted above, are general in nature and give rise to controversy in international legal forums of the highest level. However, in addition to this, the specificity of cyberspace is determined by a number of features related to its organisation and functioning, which affects security issues. In general, the term "cyberwar" is used for potentially dangerous operations in cyberspace, i.e. a war that takes place in and through computers, in digital networks that connect them, and in which states or their proxies participate against other states (Roscini, 2016; Paziuk, 2022). Cyber

warfare is usually waged against adversaries' governmental or military digital networks to damage, destroy, or block their use.

If we consider this concept in the context of international law, cyber warfare covers the means and methods of conducting military operations directed against computers or through computers and computer networks by means of information flow, when such operations in cyberspace are carried out in the context of an armed conflict defined in accordance with international law. Thus, the concepts of "cyberwar" and "cyber military threats" express a smaller scope compared to "information warfare" and "information operations".

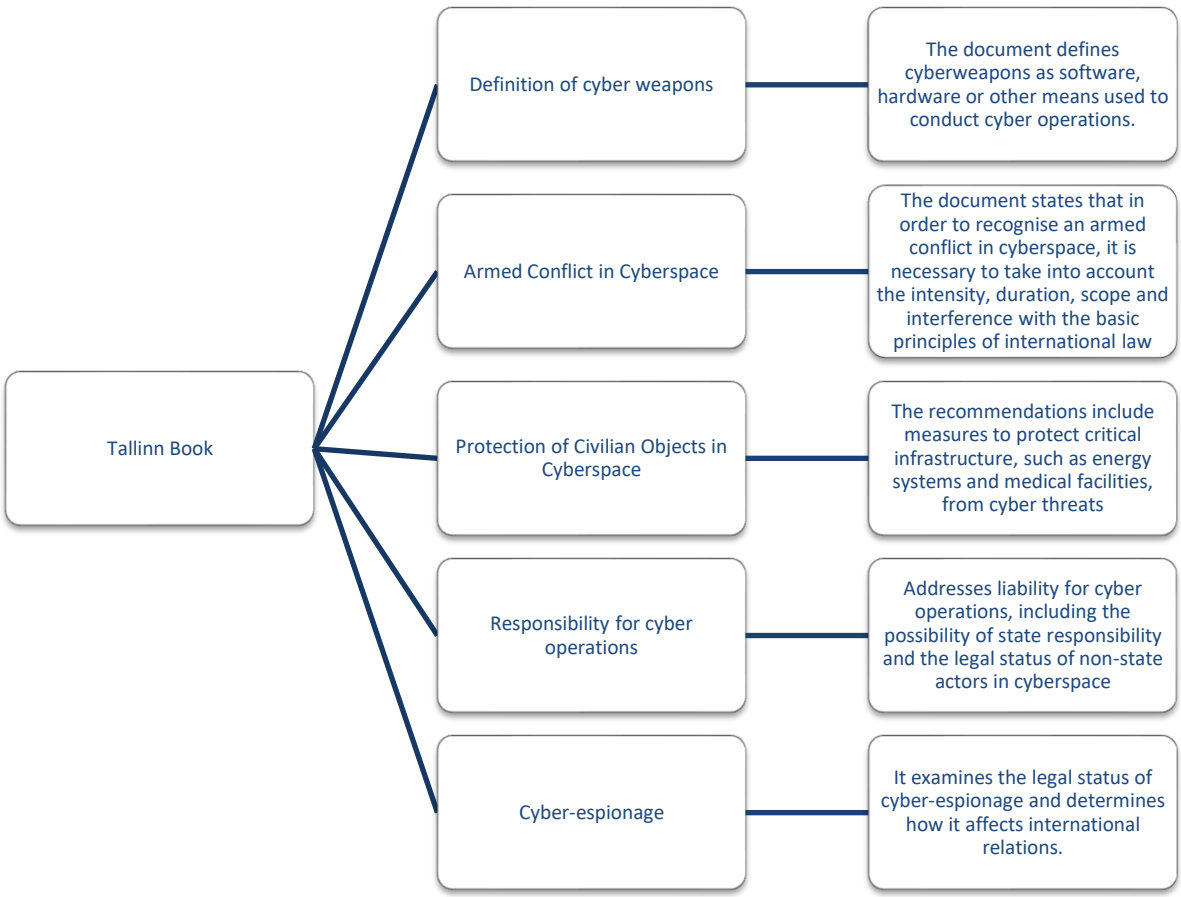
At the same time, it is difficult to determine the beginning of cyber warfare, if it is planned as a separate act. A specific problem related to the "intangibility" of information and cyber impacts is their potential importance in terms of damage caused, while they may remain "invisible" (Zahra & Wulan Christianti, 2021). For example, disabling an important infrastructure or military facility by blocking the control processors with a special programme is different from physical damage, although the consequences can be just as large. Any act of violence against the enemy, whether committed in the course of offence or defence, is regarded as an attack under Additional Protocol I to the Geneva Conventions (Article 49). Thus, cyber means may also be used as a tool, especially as it relates to military operations that may cause harm to the civilian population (Kelic, 2019). However, in this case, it may not be a matter of physical damage to such objects, but of loss of their functionality. In addition, the possibility of identifying the persons involved in a cyber-attack remains an important issue, which distinguishes such an attack from a conventional military attack, when the identification of participants is quite real (Kleemann, 2021). This creates serious problems for identifying the perpetrators and, accordingly, establishing responsibility for the actions taken, as cyber operations are very often carried out anonymously, using the power of the Internet. A "cyberattack" is defined as a hostile act aimed not only at causing damage to vital cyber systems but also to other infrastructure related to the use of the cyber system. Based on this, researchers define a cyberattack as any action aimed at undermining the functions of a computer network for political or national security purposes.

Additionally, the same Geneva Conventions protocol (Article 51) prohibits indiscriminate attacks, which arises from the difficulty of focusing cyber operations on clearly defined objects. Differences in the identification of specific objects and individuals in cyberspace, as compared to traditional conflicts, make it difficult to improve mechanisms for identifying specific perpetrators. In addition, significant damage can occur as a result of cyber operations, as the universality of the Internet and the interconnectedness of all its components make it impossible to guarantee the selectivity of an attack (Buchan & Tsagourias, 2012). This is important to take into account, as an attack on military targets may "incidentally" affect civilian networks and their users, leading to unpredictable consequences for their functioning. Such scenarios pose great challenges for ensuring that international law interacts with real-life situations in cyberspace.

The term "cybercrime" is also used to classify cyber threats. Although certain aspects of its use are widely recognised in the academic world, a precise definition is not available. One notable feature is that cybercrime is usually committed by non-state actors using computer systems, and their actions must be in violation of a state's criminal law or international criminal law (Yeboah-Ofori & Opoku-Boateng, 2023). The focus is not on undermining the functionality of a computer network, and it does not necessarily serve political or national security purposes.

The Tallinn Book as a Potential Tool for Legal Interpretation of Cyber Threats at the International Level

NATO member states have their own ideas about the legal regulation of cyber warfare threats. In May 2008, the NATO Cyber Defence Centre of Excellence (CCDCOE) was established in Tallinn. At the end of 2009, the Centre brought together an international group of lawyers and practitioners to develop a handbook to clarify the application of existing international law, including the law of war and international humanitarian law, in the context of cyber operations and cyber warfare. In April 2013, the first edition, known as the Tallinn Book, was published. In fact, the Tallinn Book is an informal collection of expert opinions and legal analyses on how existing international law applies in the context of cyber warfare and conflict (Schmitt, 2013). Figure 1 outlines the main principles of this document.



Source: compiled by the author.

The Tallinn Book attempts to define the legal principles and norms that should govern the actions of states in cyberspace. It addresses issues such as the definition of cyber-attacks, self-defence in cyberspace, the application of the principle of non-use of force, and other aspects of international law in the digital environment (Chirita, 2021). Although the Tallinn Book is not a legally binding document, it plays an important role in shaping the understanding and development of international law in the context of cybersecurity.

According to the first aspect, the international group of experts clearly rejects any claims that cyberspace is a new domain for international legal regulation. On the contrary, they point to the application of general principles of international law to this space (Pipyros et al., 2018). Regarding the second aspect, the concept of "cyber sovereignty", it is determined that no state can claim sovereignty over cyberspace in general (Pratama & Bamatraf, 2021). However, each state can exercise sovereign rights over any cyberspace infrastructure located on its territory, as well as control activities related to this cyber infrastructure. The logical conclusion is that a state's cyber operation directed against a cyber infrastructure located in another country may violate that country's sovereignty. The criterion for such a violation is harm, although the international group of experts did not reach a consensus on whether the deployment of malware that does not cause physical harm (e.g., when used to monitor activities) can be considered a violation of sovereignty (Kuusisto et al., 2020). In addition, a cyber operation may be classified as an "armed attack", triggering the right to personal or collective self-defence. Actions that are not considered an armed attack but still violate international law may also entitle the target state to take countermeasures.

Obviously, other rules of jus in bello should also apply to cyber operations, including the principles of targeting specific targets and objects, the prohibition of "fan" attacks that may affect civilians, as well as restrictions on attacks on objects essential to the survival of civilians (medical facilities, food stores, housing, and communal facilities) and incidental attacks on non-combatants (Green, 2015; Dumberry, 2019). In addition, states are responsible for cyber operations conducted against other countries from their territory. This applies even if such operations are not carried out by intelligence services, but the state provides support to those who carry out attacks on other countries.

In 2017, international law experts developed a new manual, the Tallinn Manual 2.0 (Chang, 2023). While the first edition focused on the most destructive cyber operations that can be compared and considered as "armed attacks", which entitles states to apply defence measures, it also covers those that occur during armed conflict (Gronowska, 2019). On the other hand, the second edition covers cyber operations rather than cyber conflicts, as was the case in the 2013 edition.

However, there are some comments from scholars on the further use of the Tallinn Book to counter cyber threats (Gruber, 2015; Crespo, 2018). First of all, in the second edition of 2017, researchers used the concept of cyber operations rather than cyber warfare or cyber conflicts (Arnold, 2020; Chang, 2023). Apparently, they were guided by the notion that cyber-attacks cannot be a real reason for the outbreak of hostilities, even in the digital environment (Buchan, 2016; Alnakeep, 2022). However, as the example of the Kremlin regime and its aggression against Ukraine has demonstrated, cyber-attacks can be used during real hostilities, be an integral part of offensive and defensive operations, and create or neutralise threats to digital infrastructure. Perhaps we should agree with Kleemann (2021) and Paziuk (2022) that we should expect a new edition of the Tallinn Book, which will take into account the experience of the Russian-Ukrainian war in the digital dimension. Another vulnerability of the Tallinn Book is that it is not legally binding (Sweet, 2014). It is a document containing recommendations on the application of international law to cyber conflicts. This uncertainty makes it difficult to use it as a specific legal standard.

Another challenge is that the Tallinn Book was drafted by experts from NATO countries, which makes its potential application problematic among states that are not members of this military-political bloc. It is easy to see that China, or the Russian Kremlin regimes will not recognise this legal international development, as they did not participate in its formation and generally do not share certain fundamental provisions of this document, in particular, the definition of the existence of

"sovereign cyberspace". The development of standards without a broad international consensus can create difficulties in their implementation. According to Maskun & Rum (2021), different states may define their own approaches to cybersecurity, making it difficult to create a unified system of norms. Some of the terms and definitions used in the Tallinn Book are subject to different interpretations (Nordström, 2019; Kuusisto et al., 2020; Kalpokiene, 2016), which leads to ambiguity in their application. For example, the concept of "armed conflict in cyberspace" can cause differences in interpretation, as the use of projectiles and missiles is still different from the use of digital information networks.

The issue of attribution, i.e. the ability to identify and attribute cyberattacks to specific actors, remains problematic. The Tallinn Book does not provide specific solutions to this aspect, which may be important for determining responsibility. Similarly, as Dienelt (2022) and Evans (2020) have identified, in cyberspace, identifying hostile actors and their actions is a difficult task. As of today, there are no clear identifications, and no specific mechanisms have been proposed to address them. It is also relevant to note that the Tallinn Book focuses on the application of existing legal norms to cyber conflicts, but it does not provide mechanisms for resolving the conflict itself or for further rehabilitation. In general, Gronowska (2019) and Thomas (2023) note a lack of response tools: no specific tools are provided for effective response to cyber threats and cyber defence. The recommendations developed focus mainly on legal aspects, which, moreover, do not contain tools for preventing cyber warfare. Therefore, the development of international standards in the field of cybersecurity and their implementation remain challenging, but it is necessary for stability and security in cyberspace.

At the same time, the main provisions of the Tallinn Book can be considered quite relevant for the conclusion of the next international treaty or convention on the non-proliferation of cyber threats. The developed legal mechanisms, if further improved, can replace the existing concepts of aggression and its new manifestations in the 21st century. It is obvious that the hybrid challenges of our time, the open expansionist ambitions of the Russian regime (potentially also of the PRC regime) will require the development of new instruments in international law that would take into account cyber threats at the level of an international problem. Although the development of such a convention will require additional time and political will of the international community, this option is quite promising for further implementation.

Discussion

The results obtained confirm the view that modern international conventions are important in countering cyber threats. Based on the analysis of international legal documents, it is determined that cyber warfare covers the means and methods of conducting military operations directed against computers or through computers and computer networks by means of information flow when such operations in cyberspace are carried out in the context of an armed conflict defined under international law. Thus, the concepts of "cyber war" and "cyber military threats" express a smaller scope compared to "information warfare" and "information operations".

The content analysis of the legal framework demonstrated that a cyberattack should be interpreted as a hostile act aimed not only at causing damage to vital cyber systems but also to other infrastructure related to the use of the cyber system. This definition emphasises the intent to attack and to cause injury or death, damage, or destruction of facilities. This statement is confirmed in a number of works by modern scholars (Choucri & Agarwal, 2022). Therefore, based on this, we agree with the statements of scientists who define a cyberattack as any action aimed at undermining the functions of a computer network for national security purposes.

The findings contradict the concept of Pratama & Bamatraf (2021), who only define cyberwar in the Indonesian sense as cyber-attacks. In this study, the term is etymologically split into two parts: cyber/cyber and war/warfare. UNTERM (the United Nations Multilingual Terminology Database) defines the full understanding of cyber warfare as "the offensive and defensive use of information and information systems to deny, exploit, corrupt or destroy information, information-based processes, information systems and computer networks of an adversary while protecting one's own. Such actions are intended to achieve superiority over military or business adversaries". For this reason, the concept of cyberwarfare cannot be compared to cybercrime, cyberespionage, and cybervandalism, even if they all share the use of cybertechnologies. A cybercrime is a criminal act using cybertechnologies to gain advantage for violating a country's national legislation.

The results of the study show that the international document The Tallinn Book in its modern versions is an important potential tool for the legal explanation of cyber threats at the international level. This is confirmed in the works of many contemporary scholars (Pratama & Bamatraf, 2021; Chirita, 2021; Gronowska, 2019).

The results also indicate that an important modern legal task is to reissue the Tallinn Book as a new document that would regulate cyberattacks in the international space. This thesis is confirmed by Kleemann (2021) and Paziuk (2022). In addition, it is determined that the legal uncertainty of this document remains a problem. Another problem identified is that it was drafted by NATO experts, which makes it difficult for non-members to apply the document, which is confirmed by Kleemann (2021). It was determined that some states, such as China and Russia, may reject these standards, and the lack of international consensus creates difficulties in their implementation.

Therefore, the data obtained contributed to a more detailed understanding of the importance of international law in determining cyber threats. In addition, given the above problematic aspects in modern legislation, the practical significance of the work is to formulate the main further recommendations for improving the existing legislation regulating the cyber sphere. Nevertheless, the main limitation of this review article based on content analysis is the selection of scientific sources only for the period from 2013 to 2023. The sample is limited to this range of years in order to analyse current legislation and trace the impact of the Russian-Ukrainian war on the development of international law. However, this limitation may affect the inclusion of older or earlier sources, which may also contain important information but are not included in the period.

Conclusions and Implications

The application of international law to cyber warfare raises a number of complex issues, which are further complicated by the peculiarities of cyberspace. First and foremost, there is the problem of identifying the parties to the conflict, as cyberattacks are not limited to state borders, and identifying their initiator can sometimes be simplified. The inability to clearly define the subject of responsibility, in particular in the case of actions by civilian employees, makes it difficult to define the conflict as a military one. According to the UN Charter, the use of force between states is limited, which does not contribute to the unification of the rules of cyber warfare at the international level. The problems of defining force in cyberspace give rise to different approaches and contradictions in legal forums. The specifics of cyberspace, in particular its organisation and functioning, add new challenges to security. While the terms "cyberwar" and "cyberattacks" are used for potentially dangerous operations in digital networks, its definition and regulation remain open questions.

It is determined that the Tallinn Book, which is an informal collection of expert opinions, addresses issues such as the definition of cyber-attacks, self-defence in cyberspace, and the application of the principle of non-use of force in the digital environment. Although it is not legally

binding, it plays a key role in shaping the understanding and development of international law in the area of cybersecurity. Two aspects of the Tallinn Book are noted: the rejection of the idea that cyberspace is a new domain for international legal regulation, and the definition of the limits of "cyber sovereignty". The document considers the possibility of violation of sovereignty through cyber operations and tries to define the criteria for such a violation. It is important to note that this document may become the basis for the next international convention that will regulate legal relations in the field of cyberspace at the international level.

Therefore, in general, new approaches and international standards are needed to effectively regulate and ensure security in cyberspace, in particular, given the peculiarities of this area and its impact on international relations. In particular, an important aspect is the improvement of the Tallinn Book with the adaptation of its norms for non-NATO states. It is about the joint work of international communities and experts to create a new document that will define the rules of responsibility for aggression in cyberspace for all actors in international relations. This convention should pay attention to the following aspects:

1 Definition of terms and classification of cyber aggressions. The convention should clearly define terms such as "cyber aggression", "cyber-attack", "liability" and others. It should also develop a common, unified classification of cyber aggressions to define different levels and types of attacks.

2. Establishment of basic attribution and liability mechanisms. The new document should include mechanisms for attribution of cyber aggressions to identify specific perpetrators. In this context, accountability mechanisms for states and non-state actors in cases of cyber aggression should also be established.

3. Protection of critical infrastructure. Include in the convention provisions on the protection of critical infrastructures from cyber aggression based on the involvement of international experts in the field of infrastructure security.

4. International information exchange and cooperation. The new document should also pay special attention to defining the main mechanisms of international information exchange and cooperation in the event of cyber aggressions. This will involve countries actively participating in joint investigations and information exchange.

In general, the recommendations can serve as a basis for the development of new international legal instruments aimed at establishing liability for cyber aggression.

Suggestions for Future Research

The issue of regulation of cyber-military threats by international law will be of great relevance for further research. The experience of the Russian-Ukrainian war has demonstrated the need for further research in the field of international law and cybersecurity, as current challenges in this context remain complex and insufficiently addressed. Among the important possible areas for further consideration, the following deserve the most attention:

1. Development of the legal status of cyberspace. It is important to investigate how international law can quickly and effectively adapt to changes in cyberspace and whether new regulations are needed to effectively regulate it. Alternatively, additions to existing international conventions could be a possible option. However, such possibilities would also require detailed scientific analysis.

2. The issue of the legal binding nature of the Tallinn Book. It is about studying the extent to which states take into account and use the recommendations of the Tallinn Book in their practice,

and whether there is a need to formalise these principles. For Ukraine, this issue is also relevant, as it concerns its integration into the political and military structures of the North Atlantic Alliance, which will require additional initiatives at the legislative level.

3. Identification of aspects of self-defence in cyberspace. Consideration of the possibilities and limitations of exercising the right to individual or collective self-defence in the context of cyber threats. This problem will expand the existing conventions on the use of self-defence in traditional warfare.

4. Development of standards for defining cyber-attacks. Attempts to standardise and unambiguously define the concept of cyber-attacks and other cyber operations for further use in international law. The legal aspects of such decisions are extremely important, as they will affect the identification of perpetrators, proving their guilt, imposing sanctions and possible subsequent rehabilitation, etc. International law will require thorough definitions and resolution of the terminological aspect. However, the adoption of the necessary decisions may be delayed in time, as the political will to make such decisions is not yet present.

5. Adaptation of jus in bello rules to cyber warfare. Future research should explore the definition of specific targets, objects, and limitations in cyberspace, similar to the rules relating to traditional armed conflict.

6. Study the interaction of potential new conventions with other international norms. Consideration of possible conflicts and interactions between the rules governing cyberspace and other areas of international law remains an urgent challenge for the philosophy of international law. Zkoerma. It is about gradually overcoming the dilemma in understanding cyberspace and the peculiarities of the legal system within it.

References

Alnakeep, H. T. (2022). Internet crimes to legal regulation. International journal of health sciences, 6(57), 48856–48876. https://doi.org/10.53730/ijhs.v6ns7.13683

Alsemairi, S. S. (2022). The Role of Digital Technologies in Combating Cyber-Trafficking in Persons Crimes. Computer and Information Science, 16(1), 49. https://doi.org/10.5539/cis.v16n1p49

Arnold, R. (2020). The Tallinn manual 2.0 on the international law applicable to cyber operations, edited by Michael N. Schmitt. International Criminal Law Review, 20(1), 155–159. https://doi.org/10.1163/15718123-02001008

Ayalew, Y. E. (2015). Cyber warfare: A new hullaballoo under international humanitarian law. Beijing Law Review, 06(04), 209–223. https://doi.org/10.4236/blr.2015.64021

Baradaran, N., & Habibi, H. (2017). Cyber warfare and self - defense from the perspective of international law. Journal of Politics and Law, 10(4), 40. https://doi.org/10.5539/jpl.v10n4p40

Boulos, S. (2017). The Tallinn manual and jus ad bellum: Some critical notes. In Cyberspace (p. 231–242). Springer International Publishing. https://doi.org/10.1007/978-3-319-54975-0_14

Buchan, R. (2016). Cyber warfare and the status of anonymous under international humanitarian law. Chinese Journal of International Law, 15(4), 741–772. https://doi.org/10.1093/chinesejil/jmw041

Buchan, R., & Tsagourias, N. (2012). Cyber war and international law. Journal of Conflict and Security Law, 17(2), 183–186. https://doi.org/10.1093/jcsl/krs016

Chang, C.-H. (2023). How does the Tallinn manual 2.0 shed light on the threat of cyber attacks against taiwan? European Conference on Cyber Warfare and Security, 22(1), 649–656. https://doi.org/10.34190/eccws.22.1.1294

Chirita, V. (2021). International Legal Documents on Preventing and Combating Terrorist Crimes. Internal Security, 13(2), 33–34. https://doi.org/10.5604/01.3001.0015.6560

Choucri, N., & Agarwal, G. (2022). Complexity of International Law for Cyber Operations. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4174494

Crespo, R. A. (2018). Currency warfare and cyber warfare: The emerging currency battlefield of the 21st century. Comparative Strategy, 37(3), 235–250. https://doi.org/10.1080/01495933.2018.1486090

Dienelt, A. (2022). Complementing the laws of armed conflict with human rights law and international environmental law. In Armed conflicts and the environment (p. 257–322). Springer International Publishing. https://doi.org/10.1007/978-3-030-99339-9_5

Di Martino, L. (2021). Fear and empathy in international relations: Diplomacy, cyber engagement and Australian foreign policy. Place Branding and Public Diplomacy. https://doi.org/10.1057/s41254-021-00211-9

Dinniss, H. A. H. (2015). The regulation of cyber warfare under the jus in bello. In Cyber warfare (p. 125–159). Routledge. https://doi.org/10.4324/9781315761565-7

Dumberry, P. (2019). Opinio juris. In The formation and identification of rules of customary international law in international investment law (p. 292–350). Cambridge University Press. https://doi.org/10.1017/cbo9781316481479.007

Fleck, D. (2013). Searching for international rules applicable to cyber warfare--a critical first assessment of the new tallinn manual. Journal of Conflict and Security Law, 18(2), 331–351. https://doi.org/10.1093/jcsl/krt011

Green, J. A. (2015). The regulation of cyber warfare under the jus ad bellum 1. In Cyber warfare (p. 96–124). Routledge. https://doi.org/10.4324/9781315761565-6

Gronowska, B. (2019). Judicial Dialogue in the Human Rights Domain. International Community Law Review, 21(5), 400–408. https://doi.org/10.1163/18719732-12341409

Gruber, A. (2015). Zero-Tolerance comes to international law. AJIL Unbound, 109, 337–341. https://doi.org/10.1017/s2398772300001707

Mohamed Hassan, S. A., & Mohamed Ali, S. A. (2023). Limitations On Warfare Methods: A Brief Examination Under International Humanitarian Law. Journal of Advances in Humanities Research, 2(4), 1–19. https://doi.org/10.56868/jadhur.v2i4.189

Kalpokiene, J. (2016). Book review: James A Green (ed.), Cyber warfare: A multidisciplinary analysis. Political Studies Review, 14(3), 431–432. https://doi.org/10.1177/1478929916653044

Karska, E., & Karski, K. (2019). Judicial Dialogue in Human Rights. International Community Law Review, 21(5), 391–399. https://doi.org/10.1163/18719732-12341408

Kelic, A. (2019). Cyber risk in critical infrastructure. ACM SIGMETRICS Performance Evaluation Review, 46(2), 72–75. https://doi.org/10.1145/3305218.3305243

Kleemann, S. (2021). Cyber warfare and the "humanization" of international humanitarian law. International Journal of Cyber Warfare and Terrorism, 11(2), 1–11. https://doi.org/10.4018/ijcwt.2021040101

Kurebwa, J., & Magumise, E. (2020). The Effectiveness of Cyber Security Frameworks in Combating Terrorism in Zimbabwe. International Journal of Cyber Research and Education, 2(1), 1–16. https://doi.org/10.4018/ijcre.2020010101

Kuusisto, T., Kuusisto, R., & Roehrig, W. (2020). Situation understanding for operational art in cyber operations. In Cyber warfare and terrorism (p. 192–206). IGI Global. https://doi.org/10.4018/978-1-7998-2466-4.ch011

Lancelot, J. F. (2020). Cyber-diplomacy: Cyberwarfare and the rules of engagement. Journal of Cyber Security Technology, 4(4), 240–254. https://doi.org/10.1080/23742917.2020.1798155

Lucas, G. (2017). The Tallinn manual. In Ethics and cyber warfare (p. 57–84). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190276522.003.0004

Maskun, M., & Rum, A. R. (2021). Cyber warfare: National security in dealing with changing method of war. Kanun Jurnal Ilmu Hukum, 23(3), 477–490. https://doi.org/10.24815/kanun.v23i3.22371

Naidoo, R., & Jacobs, C. (2023). Cyber Warfare and Cyber Terrorism Threats Targeting Critical Infrastructure: A HCPS-based Threat Modelling Intelligence Framework. European Conference on Cyber Warfare and Security, 22(1), 311–318. https://doi.org/10.34190/eccws.22.1.1443

Nordström, C. (2019). The Regulation of Cyber Operations Below the Threshold of Article 2(4) of the Charter: An Assessment of Rule 4 of the Tallinn Manual 2.0 [Thesis, Uppsala universitet, Juridiska institutionen]. http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-383921

Orr, Z. R. (2023). Redress for unlawful cyber-attacks during armed conflict: The limits of the international criminal court and how human rights bodies can help close the gap. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4422358

Pang, S., & Li, Y. (2020). Artificial intelligence techniques for cyber security applications. International Journal of Advanced Information and Communication Technology, 89–94. https://doi.org/10.46532/ijaict-2020021

Paziuk, A. (2022). World cyber warfare, humanism, and international law. Ukrainian Journal of International Law, 3, 43–51. https://doi.org/10.36952/uail.2022.3.43-51

Peresada, O. (2021). Qualification of crimes against life: Comparative legal analysis. Ukrainian Polyceistics: Theory, Legislation, Practice, 1(1), 61–67. https://doi.org/10.32366/2709-9261-2021-1-1-61-67

Pipyros, K., Thraskias, C., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. Computers & Security, 74, 371–383. https://doi.org/10.1016/j.cose.2017.04.007

Pratama, B., & Bamatraf, M. (2021). Tallinn manual: Cyber warfare in Indonesian regulation. IOP Conference Series: Earth and Environmental Science, 729(1), 012033. https://doi.org/10.1088/1755-1315/729/1/012033

Richemond-Barak, D. (2023). International Law and Proxy Wars. In Routledge Handbook of Proxy Wars (p. 85–99). Routledge. https://doi.org/10.4324/9781003174066-8

Roscini, M. (2016). Military Objectives in Cyber Warfare. In Ethics and Policies for Cyber Operations (p. 99–114). Springer International Publishing. https://doi.org/10.1007/978-3-319-45300-2_7

Schmitt, M. N. (Ed.). (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. https://doi.org/10.1017/cbo9781139169288

Simović, M., Rašević, Ž., & M. Simović, V. (2020). Cyber warfare and international cyber law: Whither? Journal of Criminology and Criminal Law, 58(3), 23–37. https://doi.org/10.47152/rkkp.58.3.2

Sweet, C. (2014). Tallinn Manual on the International Law Applicable to Cyber Warfare. Europe-Asia Studies, 66(4), 669–670. https://doi.org/10.1080/09668136.2014.897423

Tanodomdej, P. (2019). The tallinn manuals and the making of the international law on cyber operations. Masaryk University Journal of Law and Technology, 13(1), 67–86. https://doi.org/10.5817/mujlt2019-1-4

Thomas, A. (2023). Analysis on Cyber Crimes and Preventive Measures. International Journal for Research in Applied Science and Engineering Technology, 11(5), 3738–3744. https://doi.org/10.22214/ijraset.2023.52481

Trezza, C. (2017). Negotiation on cyber warfare. In Cyberspace (p. 257–264). Springer International Publishing. https://doi.org/10.1007/978-3-319-54975-0_16

Tsagourias, N. (2013). The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force. In Yearbook of International Humanitarian Law Volume 15, 2012 (p. 19–43). T.M.C. Asser Press. https://doi.org/10.1007/978-90-6704-924-5_2

Valuch, J., Gábriš, T., & Hamuľák, O. (2017). Cyber attacks, information attacks, and postmodern warfare. Baltic Journal of Law & Politics, 10(1), 63–89. https://doi.org/10.1515/bjlp-2017-0003

Yeboah-Ofori, A., & Opoku-Boateng, F. A. (2023). Mitigating cybercrimes in an evolving organizational landscape. Continuity & Resilience Review, 5(1), 53-78. https://doi.org/10.1108/crr-09-2022-0017

Zahra, I., & Wulan Christianti, D. (2021). The beginning of the international humanitarian law application to cyber attack: The status of rule 30 tallinn manual 1.0. Padjadjaran Journal of International Law, 5(1), 98–113. https://doi.org/10.23920/pjil.v5i1.366