Міністерство освіти і науки України
Національний університет «Києво-Могилянська академія»
Факультет правничих наук
Кафедра міжнародного та європейського права

Магістерська робота

освітній ступінь – магістр

на тему: «ВІДПОВІДАЛЬНІСТЬ У ЦИФРОВУ ЕПОХУ ЗБРОЙНИХ КОНФЛІКТІВ: ПРАВА ЛЮДИНИ ТА МЕЖІ МІЖНАРОДНОГО КРИМІНАЛЬНОГО ПРАВА»

англійською мовою

Виконала: студентка 2-го року навчання,
Спеціальності
081 Право

Васильєва Анастасія Вікторівна

Керівник: Бусол К. І.,
кандидатка юридичних наук, доцент

Рецензент _____

Магістерська робота захищена
з оцінкою _____

Секретар ЕК _____
«_____» _____20____р.

Київ – 2026

Ministry of Education and Science of Ukraine
National University of "Kyiv-Mohyla Academy"
Faculty of Law
Department of International and European Law

Master's Thesis
Education degree – Master

on the topic: «**ACCOUNTABILITY IN THE ERA OF CYBER WARFARE: HUMAN RIGHTS AND THE LIMITS OF INTERNATIONAL CRIMINAL LAW**»

Prepared by: 2nd year student
Field of Study
081 Law

Anastasiia Vasylieva

Supervisor: Kateryna Busol,
PhD in Law, Associate Professor

Reviewer: _____

Master's Thesis is defended
with a grade _____

Secretary of EC: _____
"____" _____20___

Kyiv – 2026

DECLARATION OF ACADEMIC INTEGRITY

Декларація
академічної доброчесності

Я, Васильєва Анастасія Вікторівна, студентка 2 року навчання магістерської програми за спеціальністю 081 Право факультету правничих наук НаУКМА, підтверджую таке:

- написана мною робота на тему «ВІДПОВІДАЛЬНІСТЬ У ЦИФРОВУ ЕПОХУ ЗБРОЙНИХ КОНФЛІКТІВ: ПРАВА ЛЮДИНИ ТА МЕЖІ МІЖНАРОДНОГО КРИМІНАЛЬНОГО ПРАВА» («ACCOUNTABILITY IN THE ERA OF CYBER WARFARE: HUMAN RIGHTS AND THE LIMITS OF INTERNATIONAL CRIMINAL LAW») відповідає вимогам академічної доброчесності та не містить порушень, передбачених п.3.1 Положенням про академічну доброчесність здобувачів освіти у НаУКМА, зі змістом якого я ознайомлена;
- я заявляю, що надана мною для перевірки електронна версія роботи є ідентичною її друкованій версії.

01.05.2026 Васильєва А.В.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS *5*

INTRODUCTION *7*

CHAPTER 1 CYBER WARFARE IN INTERNATIONAL LAW *11*

1.1 Cyber warfare: domain, actors, and means **11**

1.1.1. Domain 11

1.1.2 Actors 17

1.1.3 Means used 19

1.2 Cyber warfare and *jus ad bellum*: challenges and approaches **21**

1.3 Challenges for state responsibility in cyberspace **27**

CHAPTER 2 HUMAN RIGHTS IN THE CONTEXT OF CYBER WARFARE *34*

2.1 The limits of traditional human rights in the digital environment: violation error **34**

2.2 Cyber attacks and critical infrastructure **39**

2.3 The human rights dimensions of cyber attacks on infrastructure: expanding the scope of harm **49**

CHAPTER 3 INTERNATIONAL CRIMINAL LAW AND CYBER CRIMES *63*

3.1 Limits of international criminal law in ensuring individual accountability for crimes committed in cyber space **63**

3.1.1 Limits within the Rome Statute 63

3.1.2. Limits in comparison to national legislation 68

3.1.3 Limits within the group and leadership responsibility 70

3.1.4 Limits within the modes of liability 71

3.2 Reinterpreting the Rome Statute in the context of cyber operations and the new OTP framework **73**

3.2.1 Pre-policy approaches to cybercrimes 74

3.2.2 OTP Policy's approaches to cybercrimes 80

3.2.3 OTP Policy's approach to evidence and attribution within cybercrimes 84

3.3 Application of the OTP framework to cyber operations against Ukrainian infrastructure **86**

3.4 Emerging models of responsibility for cyber crimes **89**

CONCLUSIONS *99*

LIST OF REFERENCES *102*

LIST OF ABBREVIATIONS

⇒ AI	Artificial Intelligence
⇒ AP I	Additional Protocol I to the Geneva Conventions
⇒ APT	Advanced Persistent Threats
⇒ ARSIWA	Articles on Responsibility of States for Interna Wrongful Acts
⇒ CERT-UA	Computer Emergency Response Team of Ukraine
⇒ DDoS	Distributed Denial-of-Service
⇒ DoD, Pentagon	United States Department of Defense
⇒ DoS	Denial-of-Service
⇒ ICC	International Criminal Court
⇒ ICCPR	International Covenant on Civil and Political Rights
⇒ ICESCR	International Covenant on Economic, Social and Cultural Rights
⇒ ICJ	International Court of Justice
⇒ ICL	International Criminal Law
⇒ ICRC	International Committee of the Red Cross
⇒ ICTC	International Criminal Tribunal for Cyberspace
⇒ ICTY	International Criminal Tribunal for the former Yugoslavia

⇒ IHL	International Humanitarian Law
⇒ NATO	North Atlantic Treaty Organization
⇒ OTP	Office of the Prosecutor
⇒ OTP Policy on CEC	Office of the Prosecutor Policy on Cyber-Enabled Crimes
⇒ Tallinn Manual 2.0	Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
⇒ UN	United Nations

INTRODUCTION

Over the past couple of decades, digital technologies have reshaped international security, states, and law in ways that were difficult to anticipate and remain difficult to fully account for. Cyberspace is no longer a domain for simple communication, it has become a detailed system where states, non-state actors, and private entities pursue strategic objectives, and whose consequences can be similar in scale and severity from those of conventional armed conflict. Attacks on critical infrastructure, such as power grids, healthcare systems, water supply networks, communications architecture, have shown a capacity to produce harm that is cascading and not always fully captured by traditional modes of legal assessment. At the same time, it would be inaccurate to suggest that international law remains silent or wholly unresponsive to these modern changes. Existing legal frameworks, including international humanitarian law, international human right law, and international criminal law, already provide a structured and, in many respects, detailed basis for regulating conduct in cyberspace. However, their analysis is needed to establish how effectively they operate in practice. The *choice of this topic* is, therefore, grounded in the need to examine not just whether international law applies to cyber operations overall, but how precisely and effectively it does so at the present stage of its development.

The *relevance of the topic* is not simply theoretical, but also practical, in the light of the Russia-Ukraine war. High-profile incidents – from attacks on Ukrainian critical infrastructure to advanced persistent threats against governmental and civilian networks – have made clear that both the frequency and sophistication of cyber operations are rising rapidly. Yet, there is still no universally accepted definition of "cyber warfare." The threshold at which a cyber operation becomes a use of force under Article 2(4) of the UN Charter remains challenged. Attribution is persistently difficult to establish. Together, these gaps create a legal environment defined by uncertainty, and create room for impunity, complicate how states respond to cyber operations, and leave affected civilian populations without effective legal remedies. Additionally, the cumulative and long-term nature of harm caused by cyber operations adds another layer of complexity. Unlike traditional forms of attack, they do not always result in

immediate or visible damage. Instead, their effects may develop gradually, for example through the degradation of systems or disruptions to essential services. As a result, it becomes necessary to reconsider how international law understands concepts such as damage and accountability in the context of the cyber environment.

The *object of this thesis* is the body of international legal frameworks, primarily international criminal law, international human rights law, and international humanitarian law, with a focus on when and how these regimes apply to cyber operations. Together, these frameworks form the core normative structure through which the international community can address conduct in cyberspace. However, their application in this context is not straightforward. Each of these bodies of law was developed with somewhat different approaches to identifying types of harm and modes of conduct, which create both conceptual and practical difficulties when they are applied to digital environments.

The *subject of the thesis*, is whether and how those frameworks are adequate to the specific characteristics of cyber operations: their non-kinetic nature, their tendency to produce systemic and cascading effects, the difficulty of establishing intent and attribution, and the range of actors involved. The focus, therefore, is not on cybersecurity from a technical perspective, but on the normative and doctrinal questions that arise when legal rules designed for a pre-digital world are interpreted in relation to digital realities.

The *aim of this thesis* is to evaluate how existing international legal frameworks engage with cyber warfare and to identify the main areas where their application remains uncertain or incomplete. Rather than treating cyber operations as entirely outside the scope of current law, the work examines how far established rules can be interpreted to address them, and where this approach begins to reach its limits. To achieve this, the thesis first clarifies the concept of cyber warfare by addressing key definitional issues that shape the legal analysis. It then shifts to existing international legal frameworks and their application to cyber operations, with a focus on their interpretation in light of the distinctive characteristics of the cyber domain. And takes into account recent policy developments and emerging institutional approaches to

cyber-enabled conduct, while applying them to the cyber operations against Ukrainian critical infrastructure.

Since the early 2010s, there has been a noticeable increase in *academic discussion* on the relationship between international law and cyber operations, with the Tallinn Manual on the International Law Applicable to Cyber Warfare remaining one of the most influential attempts to interpret existing legal rules in the context of cyberspace. It adopts a largely conservative approach, arguing that current international law can, in principle, be applied to cyber operations through interpretation rather than requiring entirely new rules. This position is reflected in the works of Michael N. Schmitt, while other scholars, including Marco Roscini and Oona A. Hathaway, have pointed to the limits of such analogies, particularly when dealing with non-kinetic and complex forms of harm. At the same time, research in international human rights law has increasingly focused on the impact of cyber operations on civilian populations, especially in relation to privacy, freedom of expression, and broader digital rights, highlighting how such harms may be indirect, cumulative, and difficult to capture within traditional legal categories. By contrast, the application of international criminal law remains less developed, largely due to challenges related to attribution, intent, and individual responsibility in a decentralized digital environment. Recent developments, including the Office of the Prosecutor's Policy on Cyber-Enabled Crimes, reflect an attempt to address these issues within the existing framework of the Rome Statute of the International Criminal Court, an approach further explored in the work of Kai Ambos and David Scheffer. Overall, while the literature has made important progress in mapping how international law applies to cyber operations, significant gaps remain, particularly in relation to the treatment of systemic harm and the conditions for individual criminal accountability.

The *methodological foundation* of the research is doctrinal legal analysis. This means systematically examining and interpreting primary legal sources, for example, treaty texts, customary international law, decisions of international courts and tribunals, and soft-law instruments, to identify the applicable rules and norms. The doctrinal method is complemented by a comparative approach, which makes it possible

to identify different national practices and interpretive positions across the different branches of international and national law. The thesis also uses case study analysis, examining documented cyber incidents, most notably operations against Ukrainian critical infrastructure, to situate the legal analysis in real factual scenarios and test how well existing frameworks perform in practice. Taken together, these approaches make it possible to engage with the existing legal framework in a more structured way, while also critically assessing its limits and considering what could be improved within them.

CHAPTER 1

CYBER WARFARE IN INTERNATIONAL LAW

1.1 Cyber warfare: domain, actors, and means

According to the Oxford English Dictionary, the earliest recorded use of the word "warfare" dates back to 1484[1]. However, considering the history of war, it can be reasonably concluded that it might have been in use much earlier. The dictionary defines it as "the activity of fighting a war, especially using particular weapons or methods."[2] After half of a millennium, it was combined with a much 'younger' word "cyber", which stands for "connected with electronic communication networks, especially the internet". As of April 2026, there is no unified legal definition of cyber warfare. It may be described as "the use of computer programs to attack, disrupt, destroy, disable, or steal anything of military, economic or general strategic value or efforts to defend against such attacks."[3] Building upon this general understanding, a clearer analysis of cyber warfare as a concept requires examining some of its main components: the domain in which such operations take place, the actors who conduct them, and the means used.

1.1.1. Domain

Whether cyberspace can be used for warfare was a matter of a much shorter time than the emergence of the term in linguistic usage. The increased value of cyberspace expanded the motives to wage cyber warfare, for the reference, the global digital economy is estimated to contribute more than 15% of global GDP, amounting to trillions of dollars annually, and the borderless quality of Internet removed the constrain of territorial war[4].As essential state systems become increasingly digitized,

---

[1] Oxford English Dictionary, under "warfare, n.," https://www.oed.com/dictionary/warfare_n.
[2] Ibid.
[3] Hanyu Chwe, "The Rise of Cyber Warfare: The Digital Age and American Decline," *Swarthmore International Relations Journal* 1, no. 1 (2016): 43.
[4] Zia Hayat, "Digital Trust: How to Unleash the Trillion-Dollar Opportunity for Our Global Economy," World Economic Forum, 2022.. https://www.weforum.org/stories/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/.

cyberspace has emerged as a domain where strategic objectives can be pursued with low cost, plausible deniability, and minimal risk of kinetic escalation.

In 2010, the Secretary General of the International Telecommunication Union, Hamadoun Touré, warned that the growing dependence of states on interconnected digital infrastructure was creating new vulnerabilities capable of destabilizing both national security and international stability[5]. He emphasized that states must begin to confront a fundamental question of contemporary international law and security policy: at what point does a cyber operation reach a threshold such that it may be regarded not merely as espionage or sabotage, but as an act amounting to a declaration of war?[6] That same year, United States Republican senator from Maine, Susan Collins stated, reflecting a broader concern within the international community, "If someone bombed the electric grid in our country and we saw the bombers coming in, it would clearly be an act of war. If that same country uses sophisticated computers to knock out our electricity grid, I definitely think we are getting closer to saying it is an act of war."[7]

The underlying concern reflected in both Touré's remarks and Collins' observation goes beyond the digital tools and instead points to the broader implications of cyberspace as an operational domain. They suggest that when activities conducted within this domain are capable of producing large-scale effects comparable to those of conventional military force, cyberspace can no longer be understood merely as a technical environment. Rather, it must be regarded as a strategic space in which actions may reach the level traditionally associated with armed conflict.

Importantly, these concerns were not limited to policymakers. Legal scholars had already begun addressing these questions at the same time. For example, Schmitt argued as early as 1999 that cyber operations could, depending on their scale and effects, qualify as a use of force under international law[8]. A similar position was argued

---

[5] International Telecommunication Union, ITU's role in implementing WSIS outcomes. ITU Council 2010 Highlights N. 3, 2010. https://www.itu.int/council/C2010/pd/highlights/apr15.html.
[6] Ibid.
[7] Pauline C. Reich, Stuart Weinstein, Charles Wild, and Allan S. Cabanlong, "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity," *European Journal of Law and Technology* 1, no. 2 (2010): 2.
[8] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,"*Columbia Journal of Transnational Law 37* (1999): 13.

by other scholars regarding the application of to Article 2(4) of the United Nations (UN) Charter cyberspace operations and how such operations should be addressed within the existing international norms[9].

There are two prevalent views on cyberspace as a warfare domain: as a separate domain or embedded in all tradition domains[10]. Some scholars conceptualize cyberspace as a separate domain, considering it having its own characteristics and strategic dynamics[11]. The anonymity that cyber space allows differs from the one in 'real' world: while identifying perpetrators can sometimes be difficult in traditional domains, forensic capabilities in the physical environment are generally far more advanced than those available in cyberspace[12].

The global scope of the Internet reflects its borderless nature. Unlike land, sea, air, or outer space, which are defined by somewhat clear geographic boundaries and governed by established territorial or jurisdictional rules, cyberspace is not confined to a specific physical location. Instead, it consists of interconnected digital networks and information systems that operate across national borders and are used in almost all spheres, from infrastructure to economy. This interconnectedness also shows that no positive control over this domain by one actor, state or non-state, is possible[13]. Therefore, it makes the state actors vulnerable as the ability to control information in digital form is significantly more difficult, when there are other state and non-state actors which operate within the same environment and possess comparable technological means.

This domain is also much more dynamic and flexible. Each new technological breakthrough, for example, artificial intelligence becomes a means that can be utilized on itself or as a part of a weapon. For example, Artificial Intelligence (AI) has already been used in automated vulnerability detection, malware development, and large-scale

---

[9] Marco Roscini, "Cyber Operations as a Use of Force," *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan (Edward Elgar Publishing, 2015): 237.
[10] Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law* 36, no. 2 (2011): 399.
[11] Eric J. Denny, "The Cyberspace Domain: Path to a New Service?". Monograph. *School of Advanced Military Studies, US Army Command and General Staff College* (2013): p. 9.
[12] A.R. Songip et al., "Cyberspace: The Warfare Domain," *World Applied Sciences Journal* 21, no. 1 (2013): 3.
[13] Ibid, 4.

disinformation campaigns, including deepfake technologies employed to manipulate public perception during armed conflicts. And it also has a low barrier of entry: cyber tools can be developed with a relatively low cost and non-state actors or criminal groups can easily participate, which creates a sort of asymmetry of actors involved in the domain. For instance, ransomware organized criminal groups have already demonstrated the ability to conduct large-scale operations affecting critical infrastructure and governmental systems[14]. This accessibility creates a form of asymmetry in the range of actors involved, where relatively small or decentralized groups can generate effects comparable to those traditionally associated with state capabilities.[15]

One of the defining characteristics of cyber operations is the difficulty of identifying clear operational boundaries.[16] The interconnected nature of cyberspace means that actions conducted within one network can have cascading effects across multiple systems and jurisdictions[17]. As a result, the limits of cyber operations are often less visible and more difficult to define than those of conventional military activities. When a missile is used to destroy a powerplant the correlation between the means used and the consequence is much more direct and evident than when a cyber operation is conducted against the technical systems controlling the same facility, which leads to the destruction or disruption of the powerplant. This indirect relationship is clearly illustrated by the Stuxnet operation, where malicious code targeted industrial control systems and caused physical damage to centrifuges without any visible use of force[18]. Similarly, cyberattacks against the Ukrainian power grid in 2015 and 2016 disrupted electricity supply by remotely manipulating control systems rather than physically destroying infrastructure[19]. In both cases, the harmful outcome, damage or disruption

---

[14] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime: Draft — February 2013*, p. 92.https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[15] Ibid, 48.

[16] United States Air Force, *Air Force Doctrine Publication 3-12: Cyberspace Operations* (1 February 2023), p. 26. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf.

[17] Ibid, 6.

[18] Samuli Haataja and Afshin Akhtar-Khavari, "Stuxnet and International Law on the Use of Force: An Informational Approach," *Cambridge International Law Journal* 7, no. 1 (2018): 3.

[19] Miles Pollard, "A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States," *Pepperdine Policy Review* 16, no. 1 (2024): 6-15.

of critical infrastructure, resulted from interference with digital systems, making the causal link between the act and its consequences less immediate and more difficult to assess compared to traditional kinetic attacks.

The other characteristic is seen in the way cyber space used by military and civilian users. In conventional conflicts, military forces typically operate using dedicated infrastructure such as military bases and weapons systems that are not available to civilians. But in cyber military operations often rely on the same networks, software, and hardware that support civilian activities.

Although, in many cases, having real life consequences, it is a completely different environment with previously mentioned characteristics that provides adversaries to conduct both offensive and defensive operations. This view is also supported by international organizations. For example, in 2016, North Atlantic Treaty Organization (NATO) recognized cyberspace as a domain of operations analogous to land, sea, air and space, affirming that cyber activities can trigger collective defense considerations under Article 5 of the North Atlantic Treaty[20]. This recognition has catalyzed developments in the legal domain, particularly by reinforcing the applicability of existing international law to cyber operations and encouraging further doctrinal clarification. It started both state practice and academic debates on key legal issues such as attribution, thresholds of harm, and the classification of cyber operations within the framework of international humanitarian law (IHL), which were later reflected the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinn Manual 2.0). In this sense, NATO's recognition did not create new law, but rather accelerated the interpretation and adaptation of existing legal norms to the realities of cyberspace.

The other view treats cyberspace as embedded within all other domains, rather than as an entirely separate environment. From this view, cyber capabilities function as an enabling layer that permeates land, sea, air and space operations. As Larry Welch, a retired United States Air Force, general explains, the traditional hierarchy of military

[20] North Atlantic Treaty Organization, "Cyber Defence," 2024. Accessed March 1, 2026. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

domains is geophysical – land surrounded by sea, sea by air, and air by space – yet cyberspace differs because it is "embedded in all domains and operation in all domains is dependent on operation in cyberspace."[21] Since activities in cyberspace as a warfare domain, such as attack and defense, are similar to those carried out in traditional domains, and technology is widely used in both, there is no doubt that they are interconnected. Cyberspace can function as a domain through which military operations can create effects that impact other domains of warfare[22]. Furthermore, modern military infrastructure depends on information and communication technologies, which means that cyber operations, if not used in, still affect systems used in traditional military environments.

It can also be argued that these two perspectives, viewing cyberspace as a separate or interconnected domain, can be merged into one and viewed as complementary, because rejecting one of these views would overlook important characteristics that define cyberspace as a domain of warfare. On the one hand, cyberspace is increasingly recognized as a separate domain of warfare due to its unique characteristics, such as its virtual nature, borderless environment, and the ability to conduct offensive and defensive operations within in[23].

On the other hand, cyberspace is also deeply embedded in traditional domains, as modern military activities on land, at sea, in the air, and in space rely heavily on digital networks, information systems, and communication technologies. A more comprehensive perspective allows to recognize that cyberspace simultaneously functions as an independent domain of warfare and as the enabling environment that supports and influences operations across the broader battlespace[24]. This thesis therefore adopts the view that these two perspectives should not be treated as mutually exclusive. Rather, cyberspace should be understood both as a distinct domain of warfare and as an environment that is inherently integrated with other operational domains. Such an approach better reflects the technological realities of modern

[21] Larry D. Welch, "Cyberspace – The Fifth Operational Domain", *Institute for Defense Analyses* (2011): 3
[22] Ibid, 3
[23] Eric J. Denny, "The Cyberspace Domain: Path to a New Service?" Monograph. *School of Advanced Military Studies, US Army Command and General Staff College* (2013): 9.
[24] Ibid, 8-16.

warfare, where cyber capabilities can produce effects within the digital or physical environment, while simultaneously influencing and supporting military operations[25].

1.1.2 Actors

The concept of cyber warfare cannot be fully understood without analyzing the actors that operate within cyber space. The characteristics of cyber space, like low barriers to entry, anonymity, global accessibility and other, enable diverse actors to participate in cyber operations whether as a separate attack or in part of the ongoing conflict.

State actors remain central participants in cyber warfare. Governments, military organizations, and intelligence agencies develop and deploy cyber capabilities as part of national security strategies and military doctrines[26]. The importance of representing state actors lies in the fact that cyber operations, legal frameworks, and governance structures are often defined by or dependent upon state authority[27]. States increasingly integrate cyberspace capabilities into their military structures. Some countries have established specialized cyber armies focused on national defense in the digital sphere. For example, United States Department of Defense (DoD, Pentagon) has a United States Cyber Command as one of its unified combatant commands that strengthens cyber capabilities of the American army and works on cyber security with a defensive approach[28]. China's Cyberspace Force continues to modify its equipment, mainly by using drones as mobile communication relays, based on Russia's communications failures in its aggression towards Ukraine[29].

In addition to state actors, cyberspace hosts a wide variety of non-state actors who participate in cyber activities. These actors may operate independently or in coordination with state interests. Non-state actors have become increasingly relevant in cyber conflict due to the relatively low cost and accessibility of digital tools. Unlike

---

[25] Larry D. Welch, "Cyberspace – The Fifth Operational Domain", *Institute for Defense Analyses* (2011): 3.
[26] Johan Sigholm, "Non-State Actors in Cyberspace Operations," *Journal of Military Studies* 4 (2013): 6-7.
[27] Giacomo De Colle, "Towards an Ontology of State Actors in Cyberspace", *Cornell University*, p. 2. https://arxiv.org/pdf/2408.01787
[28] United States Cyber Command, "Mission and Vision," *U.S. Cyber Command*, n.d. https://www.cybercom.mil/About/Mission-and-Vision/
[29] Thomas He and Ying Yu Lin, "Cyberspace Force Equipment at the 2025 Military Parade," *China Brief Notes*, Jamestown Foundation, 10 January 2025. https://jamestown.org/cyberspace-force-equipment-at-the-2025-military-parade/

conventional military operations, cyber actions can be conducted using software and internet infrastructure that are available to nearly anybody[30]. This can be illustrated by ransomware groups such as DarkSide, which was responsible for the 2021 Colonial Pipeline attack, when being a small non-state actor using commercially available malware and infrastructure it was still able to disrupt critical energy supply chains in the United States[31]. This accessibility allows individuals and small groups to conduct operations that can affect government institutions, private corporations, and critical infrastructure. These non-state actors include "hacktivists" (actors who conduct cyber operations in pursuit of political or social objectives), cybercriminal organizations and independent hackers, but each category differs in terms of motivations, targets, and operational methods[32].

What differs the cyber domain actors from all the traditional ones is the development of new actors. AI systems are already being used for tasks such as automated vulnerability detection, network intrusion analysis, malware generation, and defensive cybersecurity operations. Moreover, on the 28th of February, 2026, OpenAI, the company that creates AI-tools, has signed an agreement with the United States DoD about their cooperation. It allows Pentagon to use OpenAI's AI systems in a closed cloud environment for its tasks (for example, analytics, operations support, information processing). In this context, AI has not (yet) become an actor in the traditional legal sense, since responsibility and decision-making authority remain with human operators, like OpenAI. But as technology gets more and more sophisticated, we might see a situation where a quasi-actor will appear, shaping the speed, scale, and methods of cyber conflict. Companies that create new means of cyber warfare or technology that can be used in this digital domain hold enough power to become separate actors, whether they will act based on their own interest or join other actors.

---

[30] Eric J. Denny, "The Cyberspace Domain: Path to a New Service?" Monograph. *School of Advanced Military Studies, US Army Command and General Staff College* (2013): 11. https://nsarchive.gwu.edu/sites/default/files/documents/2917523/Document-05.pdf

[31] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape for Ransomware Attacks* (2022): 33. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Ransomware%20Attacks.pdf

[32] Johan Sigholm, "Non-State Actors in Cyberspace Operations," *Journal of Military Studies*, no. 4 (2013): 14.

The classification of actors in cyberspace is complicated by the fluid nature of digital environments and its rapid development. Actors may shift roles over time, collaborate across organizational boundaries, or simultaneously pursue multiple objectives. And most unique of all, we might be watching new actors emerging.

1.1.3 Means used

The range of technological means used in cyber warfare is very different and they can be often hidden in plain sight. Unlike traditional warfare, where physical weapons cause almost immediate destruction, cyber warfare primarily employs software-based tools and digital techniques that can infiltrate networks and manifest its effects long after. That is how malware works, one of the most widespread mean of cyber warfare. It is a malicious software designed to damage or compromise computer systems and networks, taking different forms, like viruses, worms, Trojan horses, and ransomware. These tools allow attackers to infiltrate systems, steal sensitive data, or disrupt operations by manipulating or destroying digital resources[33].

Another widely used method in cyber warfare is the denial-of-service (DoS) attack, in which attackers overwhelm a system or network with a large volume of traffic, rendering it unable to function properly. When such attacks are conducted simultaneously from multiple compromised devices, they are called a distributed denial-of-service (DDoS) attacks. These attacks are frequently used to disrupt government services, financial institutions, or even critical infrastructure.

Cyber operations may also involve advanced persistent threats (APTs), which are highly sophisticated and long-term cyber campaigns aimed at gaining continuous access to targeted systems. APT operations are typically carried out over extended periods and are often associated with state-sponsored cyber activities aimed at espionage or strategic disruption[34].

There are numerous ways of how the cyberspace, or its technological means can be used as cyber weapons. Since cyber space as a domain can exist both separately and embedded into physical domain, the cyber weapons that are being used and developed

[33] Nuran Mahmudov, "Cyber Warfare: Understanding the Elements, Effects, and Future Trends of Cyber-Attacks and Defences," *Security & Defense*, no. 2 (2023): 38.
[34] Ibid, 40.

can also become a part of other physical weapons. Modern military platforms, including drones, communication systems, and advanced weapons systems, rely heavily on digital networks and software-based control mechanisms. As a result, cyber weapons should not be viewed only as independent tools operating exclusively in the digital domain, but also as weapons that may complement or integrate with traditional forms of warfare. The continuing development of digital technologies and the increasing dependence of military systems on networked infrastructure suggest that future conflicts may involve even closer interaction between cyber capabilities and conventional military force.

In response to such technological capabilities, international discussions have taken place within the framework of the Convention on Certain Conventional Weapons, particularly regarding so-called Lethal Autonomous Weapons Systems. Many states and experts, along with the International Committee of the Red Cross (ICRC), have emphasized the importance of maintaining "meaningful human control" over the use of force, especially when advanced technologies such as artificial intelligence are incorporated into weapons systems[35]. So, with such fast and wide possibilities for the incorporation of cyber weapons and cyber systems into the traditional warfare domain, rises a need for legal control.

Considering the comprehensive nature of cyber warfare, it can be argued that the concept itself can be a separate topic for a much deeper analysis. However, even this superficial analysis shows how closely intertwined it is with traditional domains of warfare and, at the same time, can be a completely separated field for an attack. Unlike traditional warfare, which has historically been dominated by states and their armed forces, cyber operations may involve both state and non-state actors, including private groups, "hacktivists", criminal organizations, and individual hackers. These actors have a wide range of cyber weapons available, from various malware to planned DDoS attacks that can have consequences outside of the online world. It is a unique domain

[35] International Committee of the Red Cross, "Views of the International Committee of the Red Cross (ICRC) on Autonomous Weapon System," background paper submitted to the CCW Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Geneva, 2016, p.5.https://www.icrc.org/en/document/views-icrc-autonomous-weapon-system

that can fastinate in both positive and negative way, as it reflects the development of our society, but also challenges traditional understandings of conflict and security. The boundaries between peace and conflict, civilian and military infrastructure, and state and non-state actors are often blurred in cyberspace. Therefore, it requires an examination of how existing *jus ad bellum* principles can be applied to such unique space.

1.2 Cyber warfare and *jus ad bellum*: challenges and approaches

Jus ad bellum, a set of legal rules regulating the legality of the use of force, is a centuries old concept. With the emergence of the new technology, it has required scholars and practitioners to reconsider how such rules can be applied within the cyber domain, taking into account the challenges that the characteristics of cyber space carry.

When referring to the use of force in the traditional domains, the baseline lies within the Article 2(4) of the UN Charter, which prohibits states from using force against "the territorial integrity or political independence of another state"[36]. It does not mention the effects or specific consequences that such use of force should cause. However, most scholars and practitioners interpret this definition as referring to armed violence between states capable of causing physical damage or loss of life[37]. This interpretation appears logical when considered in the context of traditional physical domains of warfare, where most uses of force result in some form of destruction to objects or loss of life. Despite a very short wording of the Article, many scholars and practitioners also understand it as prohibition of "any use of force not otherwise permitted by the terms of the Charter, specifically uses of force authorized by the Security Council and defensive operations"[38]. Rule 68 of the Tallinn Manual 2.0, also proposes a prohibition of threat or use of force in connection to the Article 2(4) of the

[36] *Charter of the United Nations*, signed 26 June 1945, entered into force 24 October 1945, art. 2. Accessed March 4, 2026. https://www.un.org/en/about-us/un-charter/full-text
[37] Erin Pobjie, "The Meaning of Prohibited 'Use of Force' in Article 2(4) of the UN Charter," *Articles of War*, Lieber Institute West Point, 2024. https://lieber.westpoint.edu/meaning-prohibited-use-force-article-24-un-charter/
[38] Michael N. Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," *Villanova Law Review* 56, no. 3 (2011): 571.

UN Charter: "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.[39]"

Yet, cyber operations challenge this traditional paradigm by lacking the forceful nature, as they are generally non-kinetic, yet their consequences may range from relatively minor disruptions to severe damage, including loss of life[40]. Therefore, scholars, when applying *jus ad bellum* to cyber warfare, resolve this problem by interpreting it through the consequences of the attack[41]. Meaning, for example, that if a cyber attack, non-kinetic in its nature, disrupted the computerized control systems of a power grid in way that led to an explosion and the destruction of infrastructure, then it can be viewed as a force. This effects-based approach also goes in line with Rule 92 of the Tallinn Manual, which sets a threshold of damage or injury for cyber operations to be qualified as cyber attacks, and the adoption of the scale-and-effects test in Rule 69.

Another interpretation suggested in legal scholarship is the target-based approach. According to this view, the classification of a cyber operation as a use of force or even an armed attack does not primarily depend on the consequences produced by the operation, but rather on the nature of the object that is targeted. In other words, the decisive factor is whether the cyber operation is directed against systems that are considered essential to the functioning of the state. This approach also has merit considering that it allows to take into account operation that were directed against specific critical targets, but attempted attacks that failed or were mild in effects. The unsuccessful outcome should not negate the underlying character of the operation. Within this framework, cyber operations targeting critical infrastructure may qualify as uses of force or armed attacks even in the absence of immediate physical destruction or loss of life[42]. The reasoning behind this approach is that attacks against such systems

---

[39] Schmitt, Michael N., ed. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd ed. Cambridge: *Cambridge University Press* (2017): 329

[40] Ibid, 340.

[41] Ibid, 329.

[42] Kai Ambos, "Cyber-Attacks as International Crimes under the Rome Statute of the International Criminal Court?," *ICC Forum*, 7 March 2022. Accessed March 6, 2026. https://iccforum.com/cyberwar#Ambos.

may seriously undermine the functioning of the state and its ability to maintain security, public order, and essential services[43].

However, the application of this approach raises an additional difficulty, namely the definition of critical infrastructure itself. International and national instruments generally describe critical infrastructure as systems whose disruption would have significant consequences for national security, the economy, or public safety. These typically include sectors such as energy generation and distribution, financial systems, transportation networks, water supply, healthcare systems, and the digital infrastructures that support their functioning. There is a position among scholars that treating any cyber intrusion as a use of force risks lowering the threshold for the lawful use of force and may increase the likelihood of escalation between states[44]. For this reason, many scholars remain cautious about adopting a purely target-based interpretation when applying *jus ad bellum* to cyber operations[45].

One more interpretation discussed in legal scholarship is the instrument-based approach, which focuses on the means used to conduct the operation. Under this view, the classification of an act as a use of force depends primarily on the type of weapon or instrument employed. Traditionally, the understanding of the use of force in international law developed within a framework in which force was closely associated with the use of kinetic weapons, such as conventional military weapons, chemical weapons, biological weapons, or nuclear weapons. Within this paradigm, an operation would qualify as a use of force when it involved the employment of instruments capable of producing destructive physical effects through the application of kinetic force. One of the advantages of the instrument-based approach lies in its predictability and clarity. Because the analysis focuses on the nature of the weapon used, the determination of whether a particular action qualifies as a use of force becomes relatively straightforward. If the operation involves the use of traditional military weapons or comparable instruments of armed violence, it may fall within the

[43] Ibid.
[44] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (2012): 846.
[45] Ibid, 847.

prohibition of Article 2(4) of the UN Charter[46]. By contrast, actions carried out through other forms of coercion, such as economic pressure or diplomatic measures, would not meet the threshold of the use of force and would instead fall within other areas of international law[47].

However, the application of the instrument-based approach to cyber operations is widely debated. Because cyber operations rely on digital tools rather than traditional weapons, they do not fit easily within a framework that associates force primarily with kinetic instruments. As a result, many contemporary scholars argue that the instrument-based approach is increasingly inadequate for analyzing modern forms of conflict[48]. While it historically shaped the interpretation of the prohibition of force, the emergence of cyber capabilities has led many commentators to conclude that focusing solely on the instrument used may no longer capture the full range of coercive actions that can occur between states.

It seems reasonable to suggest that the assessment of cyber operations under *jus ad bellum* should not be confined solely to the weapons used or their immediate physical effects. From this perspective, the decisive question may be not only what consequences the operation produces, but also whether the operation functions as a coercive instrument of warfare against another State. Such a character-based approach would allow some cyber operations to be viewed as force even without reducing their analysis simply to the physical-style effects. In particular, cyber operations directed at disabling military capabilities, neutralising air defence systems, paralyzing command-and-control structures, or otherwise undermining a State's ability to exercise control over essential governmental or strategic functions may resemble traditional uses of force in their military character and strategic purpose, even where no immediate destruction is visible.

There is also a position among scholars that adopting such an interpretation raises a need for limitations, because if force is understood too broadly other forms of

---

[46] Ibid, 842.
[47] Ibid, 842.
[48] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,"*Columbia Journal of Transnational Law 37* (1999): p 15.

it, like economical pressure, might become qualified for the use of force[49]. This reasoning appears convincing, that is why a non-consequences-based approach would still require limiting criteria. This thesis suggests that these can include the military character of the operation, its direct connection to hostile state action, or its capacity to disable or neutralize essential state functions. In this way, cyber force could be understood more broadly than physical destruction alone, while still remaining distinct from mere political, economic, or informational coercion.

While the character-based approach may also be criticized for its potential lack of precision, the appeal of the effects-based approach lies in its relative simplicity: physical harm is easier to identify than the strategic character of a cyber operation or its connection to hostile state action. Nevertheless, an approach that relies exclusively on physical consequences risks creating a grey zone in which significant cyber operations are disregarded merely because they do not produce immediate physical damage. That creates a ground for manipulation, allowing states to design cyber operations in a way that avoids immediate physical harm while still achieving coercive strategic objectives. And while it might sound sci-fi and somewhat speculative in 2026, the legal scholarship has to be prepared for the increasingly sophisticated use of cyber capabilities capable of disrupting essential state functions without producing traditional physical destruction in the near future.

Such diversity of approaches shows that the unique characteristics of the cyber domain challenge modern *jus as bellum* and demonstrate that not all rules of international law can be directly applied to cyber warfare.

Another challenge that the cyber warfare created for the application of the *jus ad bellum* is the self-defence problem, particularly the threshold that is now set in a way that exclude many cyber operation that are harmful in a non-physical way. As Article 51 the UN Charter permits self-defence only in response to an armed attack, the International Court of Justice (ICJ) clarified in the Military and Paramilitary Activities in and against Nicaragua that armed attacks represent the “most grave forms” of the use of force, distinguished from less severe uses of force by their scale and

[49] Ibid, 16-17.

effects[50]. The 2011 U.S. International Strategy for Cyberspace states that, in line with the United Nations Charter, countries possess an inherent right to self-defense, which may be invoked in response to certain hostile actions conducted in cyberspace[51]. However, applying it to cyber operations, has proven difficult. According to the Rule 92, as it was mentioned before, the creators of the Tallin Manual 2.0 preferred the effect-based approach. But some scholars believe that, not just in terms of qualifying a cyber operation as a use of force, but also in terms of self-defense, such approach becomes faulty[52]. Many cyber operations may involve significant disruption without producing the physical destruction traditionally associated with military force, making it difficult to determine whether the threshold of force has been crossed. And, in the result, such approach denies the right to self-defense. It is also important to note that it is both the scale and the effects of the cyber attack that are taken into account when determining that the cyber attack occurred. For example, a large-scale DDoS attack conducted through millions of compromised devices may temporarily disrupt national critical infrastructure and be substantial in scale, but not cause any physical harm, therefore, disregarded.

This argument also mirrors the position of some states. For example, the DoD's in its Assessment of International Legal Issues suggested that a state may have the right to act in self-defence if a cyber operation causes serious damage to important computer systems or the data stored within them, particularly when those systems are essential for national security or critical infrastructure[53]. The assessment somewhat combines the effects-based and character-based approaches, as it expands the effects beyond the classical physical world damage and notes that the broader context of the operation and

---

[50] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, I.C.J. Reports 1986, para. 191. https://www.icj-cij.org/case/70

[51] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (May 2011): 10 . https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[52] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (2012): 846-847.

[53] United States Department of Defense Office of General Counsel, "An Assessment of International Legal Issues in Information Operations," appendix in *Computer Network Attack and International Law*, *International Law Studies*, vol. 76, ed. Michael N. Schmitt and Brian O'Donnell (US Naval War College, 2002): 487. https://digital-commons.usnwc.edu/ils/vol76/iss1/4/.

the attacker's clearly malicious intent is also relevant. Roscini addresses the concerns of critics by highlighting that even if a cyber operation qualifies as an armed attack under such broader approach, this does not automatically allow the victim state to use force in self-defence, since any response must still satisfy the requirements of necessity and proportionality[54].

Such debates suggest that a threshold tied exclusively to only observable, traditional physical effects may fail to capture the full range of harmful cyber operations. A more context-sensitive assessment that considers the nature, purpose, and strategic character of the operation may therefore provide a more adequate framework for evaluating cyber attacks within the existing *jus ad bellum* regime. At the very least, if the effects-based approach is considered preferable for reasons of legal certainty, the concept of "effects" should be adapted to include non-physical, but still substantial, consequences arising from cyber operations.

1.3 Challenges for state responsibility in cyberspace

One of the challenges in applying *jus ad bellum* to cyber warfare, that was not included in the precious subchapter, is the difficulty of attributing cyber operations to a specific state. Attribution is examined in this subchapter on state responsibility, since it determines whether a particular cyber operation can be legally attributed to a state.

In international law, state responsibility refers to the legal consequences that arise when a state commits an internationally wrongful act. Unlike domestic legal systems, international law does not operate with a classical criminal code where states can be prosecuted or punished in the same way as individuals. In other words, there is no equivalent of a Criminal Code for states, and international law does not impose criminal liability on states themselves. Instead, the concept of state responsibility functions as a framework that determines when a state has violated an international obligation and what legal consequences follow from that violation.

---

[54] Roscini, Marco. "Cyber Operations and the Use of Force in International Law". Oxford University Press, (2014): 121.

The modern understanding of state responsibility is largely reflected in the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), which, although not a treaty, are widely regarded as an authoritative codification of customary international law. According to this framework, two basic elements must be established in order for a state to incur responsibility. First, the conduct in question must be attributable to the state[55]. This means that the act must have been carried out by state organs, persons or entities acting on behalf of the state, or actors whose conduct can otherwise be legally linked to the state. Second, the conduct must constitute a breach of an international obligation binding upon that state[56]. In other words, the state must have failed to comply with a rule of international law that applies to it.

If both of these elements are present, the act qualifies as an internationally wrongful act, and the state incurs responsibility. However, this responsibility does not function as criminal punishment. Rather, it creates legal obligations for the responsible state, such as the duty to cease the wrongful conduct, provide assurances of non-repetition, and make reparation for the damage caused. In this sense, state responsibility operates more as a system of legal accountability and restoration than as a system of criminal liability.

Unlike conventional military attacks, cyber operations are often conducted through complex technical infrastructures that allow perpetrators to conceal their identity, route attacks through multiple jurisdictions, or rely on proxy actors. The attribution problem has two main dimensions: a technical dimension and a legal dimension[57].

The technical problem concerns identifying the true origin of the cyberattack and determining who actually carried it out. Unlike traditional military attacks, cyber operations can be launched through many different computers and networks located across the world. Attackers can route their actions through multiple machines and

---

[55]International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (2001), Art. 2. Accessed March 10, 2026. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

[56] Ibid, Art. 2.

[57] Lorraine Finlay and Christian Payne, "The Attribution Problem and Cyber Armed Attacks," *AJIL Unbound* 113 (2019): 202.

jurisdictions, which makes tracing the real source of the attack extremely difficult. Because cyberspace has no clear physical borders and allows for a high level of anonymity, perpetrators can hide their identity or even intentionally mislead investigators about where the attack originated. These technical characteristics create serious challenges for states. Cyberattacks often take a long time to detect and investigate, and establishing a reliable forensic connection between the attacker and the incident may require extensive technical analysis and intelligence information. In some cases, states may also be reluctant to reveal the intelligence capabilities they used to identify the attacker. As a result, determining the origin of a cyberattack can take months rather than hours or days. The technical difficulties of attribution can also create a risk of misattribution[58]. If a state incorrectly identifies the source of an attack, it may respond against the wrong actor, potentially escalating international tensions or even triggering armed conflict. At the same time, the time required to identify the responsible party may undermine the immediacy requirement of self-defence in international law, which traditionally requires a prompt response to an armed attack.

The second dimension of the attribution problem is the legal question of state responsibility. Even if investigators are able to determine who carried out the cyberattack, it must still be established whether that conduct can legally be attributed to a state. Under international law, states are responsible for acts carried out by their organs or by individuals acting under their direction or control. However, many cyber operations are conducted by private individuals or loosely organised hacker groups rather than official state actors. This creates additional legal complexity because attributing the actions of non-state actors to a state usually requires a high threshold of proof.

Two competing legal standards have developed for attributing responsibility to states for acts carried out by non-state actors: the effective control standard and the overall control standard. The effective control test, developed by the International Court of Justice in the Nicaragua case, requires that a state exercise complete operational control over the actors committing the attack in order for their conduct to

[58] Ibid, 203.

be attributed to the state[59]. By contrast, the overall control test, formulated by the International Criminal Tribunal for the Former Yugoslavia (ICTY) in the *Tadić* case, considers a state responsible when it organizes, coordinates, or supports a group carrying out the attack, even if it does not direct every specific operation[60].

There are scholars who argue that the effective control standard imposes an extremely high burden of proof, particularly in the cyber context where the anonymity and technical complexity of cyber operations make it very difficult to identify the perpetrators with certainty[61]. As a result, applying this strict standard could allow states to sponsor cyber attacks while maintaining plausible deniability and avoiding accountability. For this reason, adopting the broader overall control standard would make it easier to hold states responsible for cyber attacks when there is sufficient evidence of state involvement[62].

A key critique of the overall control test concerns its limited acceptance within the law of state responsibility. Although the test, developed by the ICTY in *Tadić*, lowers the threshold for attribution by requiring only that a state exercise a degree of authority over non-state actors, such as coordinating or supporting their activities, it remains controversial in interstate disputes[63]. Furthermore, the ICJ has expressed concern that the overall control test risks expanding state responsibility beyond the fundamental principle that states are responsible only for their own conduct. By allowing attribution based on general coordination or support, the test may blur the distinction between state actions and the independent conduct of non-state actors. The International Law Commission has similarly emphasized that the overall control test was developed primarily in relation to individual criminal responsibility, not state responsibility under international law. In the cyber context, these concerns are further

---

[59] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, I.C.J. Reports 1986, para. 112. Accessed March 10, 2026. https://www.icj-cij.org/case/70

[60] *Prosecutor v. Duško Tadić*, Case No. IT-94-1-A, Judgment (ICTY Appeals Chamber, 15 July 1999), para. 131-145. Accessed March 12, 2026. https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf

[61] Scott J. Shackelford, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem," in *Proceedings of the 2010 Conference on Cyber Conflict*, ed. C. Czosseck and K. Podins, CCD COE Publications, (2010): 201-202.

[62] Ibid, 203-204.

[63] Zhifeng Jiang, "Regulating the Use and Conduct of Cyber Operations through International Law: Challenges and Fact-finding Body Proposal," *LSE Law Review* 5 (2020): 63.

reinforced by the strategic advantage of plausible deniability: states rarely issue explicit instructions or publicly endorse cyber operations carried out by non-state actors. As a result, even the lower threshold of overall control may remain difficult to demonstrate in practice, while at the same time raising doctrinal concerns about over-expanding the scope of state responsibility[64].

If the effective control test is too strict, and the overall control risks of being too broad, then a more realistic approach may therefore require a hybrid attribution model that combines elements of control with contextual indicators of state involvement. Rather than relying exclusively on formal instructions or hierarchical control, such a framework could consider the broader operational environment, patterns of coordination, and the strategic interests served by the cyber operation. Another option, is also a negligence-style responsibility model, whereby states incur responsibility where they knew or reasonably should have known that harmful cyber operations were being conducted from infrastructure within their jurisdiction. However, a popular approach is applying a principle of due diligence. Under this principle, states have an obligation not to allow their territory or infrastructure to be used in a way that causes harm to other states. In the cyber context, this means that states must take reasonable steps to prevent malicious cyber activities conducted from networks or systems within their jurisdiction[65]. It is vital to understand that this duty does not require states to guarantee that no cyber attacks originate from their territory, but rather to exercise reasonable vigilance and take appropriate measures when they know or should reasonably know about harmful activities[66]. Importantly, due diligence functions as a duty of best efforts, meaning that the expected level of prevention depends on the technological capabilities and resources of each state, because what is considered reasonable for a technologically advanced state may differ from what can be expected from a less developed one[67].

---

[64] Ibid, 64.
[65] Schmitt, Michael N., ed. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." 2nd ed. Cambridge: *Cambridge University Press*, (2017): 30-43
[66] Ibid, 30-43.
[67] Jan Martin Lemnitzer, "Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace," *European Journal of International Law* 33, no. 3 (2022): 794-795.

Taken together, it is clear that state responsibility for cyber operations remains difficult to establish due to limitations of the existing tests and the lack of clear consensus on whether other principles or new tests should be developed to fit the characteristics of cyber space.

***

Cyber warfare is a fundamental challenge for the international law and *jus ad bellum* norms in and of itself. It changes the way legal scholars understand conflict, armed attack and warfare. The characteristics of cyberspace, among which are anonymity, lack of clear geographical and operational boundaries, flexibility and other, as a domain of warfare reveal a unique operational environment that can both be used as a separate independent arena of conflict and as a supporting component of traditional military operations. The diversity of actors – including states, proxy groups, and private individuals – combined with the dual-use nature of cyber tools, further complicates attempts to categorize cyber operations within existing legal frameworks. Considering the changing and transforming nature of technology, it is possible for new actors, for example AI corporations, to appear in the near future as separate and influential participants of cyber operations.

The application of *jus ad bellum* also raises important legal and conceptual questions. Traditional approaches, particularly the instrument-based model, appear inadequate in capturing the realities of cyber conflict, where non-kinetic means may nevertheless produce significant strategic and societal harm. As a result, there has been a gradual shift toward effects-based and scale-and-effects approaches, which better reflect the functional impact of cyber operations. However, there is also a character-based approach that requires an assessment of the nature and purpose of the operation, focusing on whether it is inherently coercive or hostile in character, regardless of its physical effects. Unfortunately, due to the lack of consensus on the definitions of important terms and thresholds, the application of existing legal frameworks to cyber operations remains inconsistent and uncertain, and requires improvements that will be able to grasp as many unique characteristics of cyber domain as possible.

In terms of state responsibility, the most profound challenge lies in the attribution of conduct to states. While the legal framework of state responsibility, as codified by the International Law Commission, formally applies to cyberspace, its practical implementation is severely constrained by technical anonymity, plausible deniability, and the involvement of non-state actors. The divergence between the "effective control" and "overall control" tests further exacerbates this uncertainty, leaving no universally accepted standard for attributing cyber operations.

Taken together, these challenges highlight the evolving nature of international law in response to the realities of cyber warfare. While existing legal doctrines were not originally designed with cyberspace in mind, international law has demonstrated a notable degree of flexibility and adaptability in extending to this new domain. The current debates and interpretative divergences should therefore be understood not as weaknesses, but as part of an ongoing process of legal development and clarification. This dynamic creates an opportunity to refine key doctrines, particularly those related to the use of force and state responsibility, to ensure their continued effectiveness and relevance in the cyber context.

CHAPTER 2

HUMAN RIGHTS IN THE CONTEXT OF CYBER WARFARE

2.1 The limits of traditional human rights in the digital environment: violation error

Before the COVID-19 pandemic, the debate on whether digital rights are exceptionally new or serve as extensions to the existing "traditional" fundamental human rights existed, but was not as prominent or urgent within legal and academic discourse[68]. Since 2020, this debate took a turn, showing how deeply rooted in the digital space our lives can be: from studying to working and even socializing online, such expanded digitalization of almost every aspect of life have underscored the need to re-evaluate how important re-evaluation of the nature of digital rights is. Although the UN Human Rights Council Resolution on the promotion, protection and enjoyment of human rights on the Internet affirms that "the same rights that people have offline must also be protected online"[69], it is important to consider that traditional architecture of human rights law was created before the evolution of digital sphere, when Facetime calls and AI systems were a part of the sci-fi books. As a result, while the normative framework remains formally applicable, its operational effectiveness is significantly strained in practice. Over the years it has become evident that digital space challenges traditional human rights law in ways that highlight the differences of how human rights are interpreted, governed, and enforced within it.

Two popular views are that any digital right is, necessarily, an extension or an adapted version of the existing fundamental law or completely new rights that are

[68] Dafna Dror-Shpoliansky and Yuval Shany, "It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology," *European Journal of International Law* 32, no. 4 (2021): 1257.
[69] UN Human Rights Council. *The Promotion, Protection and Enjoyment of Human Rights on the Internet*. HRC Res. 20/8. UN Doc. A/HRC/RES/20/8. 16 July 2012, para. 1. https://digitallibrary.un.org/record/731540?ln=en&v=pdf

designed specifically for the digital space and cannot be used outside of it[70]. However, there is a more nuanced way of approaching such debate, which combined these two views without underestimating any of them[71]. Considering the UN Human Rights Council's affirmation that people should enjoy the same rights online as they do offline, traditional human rights still remain the starting point for many digital rights. Since new technologies require us to reinterpret existing rights, such as freedom of expression and the presumption of innocence, in light of digital realities, many digital issues are dealt with through the adaptation of existing rights, not through abandoning them[72]. For example, browsing history, device tracking, and private communications are generally understood as new forms of interference with the existing right to privacy, not as a separate digital right[73].

However, considering the technological development and how different digital space can be from the offline world, it has not only introduced new ways of approaching traditional rights, but also produced new rights and freedoms. Among those proposed new rights that do not correspond with any of the existing fundamental rights is a right of access to the Internet[74]. Another example is a right not to be subjected to automated decision-making in significant matters, which is connected to an even newer debate about human rights within interactions with the AI systems[75]. These rights are linked to the underlying values and objectives of fundamental rights – such as human dignity, autonomy, and effective participation in society – but they do not directly derive from any single pre-existing right. Rather, they emerge as responses to novel technological conditions that expose gaps in the traditional human rights framework, requiring more tailored normative protections. AI systems have become so

---

[70] Tiina Pajuste, "Adapting Human Rights to a Digital World," in *Human Rights in the Digital Domain: Core Questions*, Cambridge University Press, (2025): 19-26.
[71] Ibid, 19-26.
[72] Jacopo Coccoli, "The Challenges of New Technologies in the Implementation of Human Rights: An Analysis of Some Critical Issues in the Digital Era," *Peace Human Rights Governance* 1, no. 2, (2017): 224.
[73] European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence*, p. 56-76. https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng
[74] Yuval Shany, "Digital Rights and the Outer Limits of International Human Rights Law," *German Law Journal* (forthcoming), Hebrew University of Jerusalem Legal Research Paper No. 23-2 (2022): 465.
[75] Elena Abrusci and Richard Mackenzie-Gray Scott, "The Questionable Necessity of a New Human Right against Being Subject to Automated Decision-Making," *International Journal of Law and Information Technology* 31, no. 2 (2023):114.

popular over the last couple of years, but not all general users understand the scale and speed of automated processes or the diffusion of responsibility for its' decisions. AI can be unpredictable and dangerous, so much so, that simply stretching traditional rights may result in insufficient protection. As a result, there is a popular argument that adaptation alone is not enough[76].

When the gap between existing rights and technological realities becomes too significant, the development of new, more specific rights becomes necessary[77]. In 2023 the Human Rights Council has already warned about the serious risks that AI systems carry and requested the Office of the High Commissioner to prepare a report mapping the gaps and challenges related to human rights within the AI usage[78]. The report reaffirmed that existing human rights apply to AI, but identified significant conceptual, accountability, and enforcement gaps in addressing issues such as algorithmic opacity and multi-actor responsibility[79]. By emphasizing the need for new mechanisms like human rights impact assessments, transparency, and human oversight, it also suggested that the mere extension of traditional rights may be insufficient to fully address the challenges posed by emerging technologies[80].

Yuval Shany interestingly suggests that there are three generations of rights: first generation of digital rights that were derived from the fundamental rights and repackaged to try to fit them into the digital world; second generation, a completely new digital rights created according to the unique characteristics of the digital sphere; and third generation tied to the new rights-holders and new duty-holders[81].

So, while the foundational stance that human rights apply equally online remains widely accepted, it becomes increasingly evident that traditional doctrines struggle to

---

[76] Tiina Pajuste, "Adapting Human Rights to a Digital World," in *Human Rights in the Digital Domain: Core Questions*, Cambridge University Press, (2025):18-24.
[77] Ibid, 18-24.
[78] UN Human Rights Council. *New and Emerging Digital Technologies and Human Rights*. HRC Res. 53/29. UN Doc. A/HRC/RES/53/29. 18 July 2023. Accessed March 17, 2026. https://docs.un.org/en/a/hrc/res/53/29
[79] UN Office of the High Commissioner for Human Rights, *Mapping Report: Human Rights and New and Emerging Digital Technologies*, UN Doc. A/HRC/56/45 (20 August 2024), Accessed March 17, 2026. https://www.ohchr.org/en/documents/thematic-reports/ahrc5645-mapping-report-human-rights-and-new-and-emerging-digital
[80] Ibid.
[81] Yuval Shany, "Digital Rights and the Outer Limits of International Human Rights Law," *German Law Journal*, Hebrew University of Jerusalem Legal Research Paper No. 23-2 (2022): 464.

address the scale, speed, and private governance structures of the digital sphere. This has led to a more nuanced understanding: digital rights may formally derive from existing human rights, yet their protection requires reinterpretation, adaptation, and, in some cases, the development of more specific normative frameworks, which are capable of responding to the realities of an increasingly digitalized world.

But no matter the approach or generation, there is another prominent problem that is less discussed – violation errors, situations in which substantial interferences with human rights in the digital sphere, or by what is happening in it, occur but are not formally recognized as violations within existing legal frameworks, because of the lesser consequences. For instance, interference with electricity grids or water supply systems that causes short-term outages may significantly affect access to essential services and, indirectly, rights such as the right to health or an adequate standard of living.

However, because such disruptions are limited in duration and do not result in lasting damage or loss of life, they often fall below the threshold required for formal legal qualification as a violation of human rights or as a prohibited use of force. Just like the kinetic and non-kinetic effects of the physical attacks and cyber attacks respectively, human rights law has traditionally focused on direct, identifiable, and often physical forms of harm[82]. As a result, the absence of visible or immediate damage can lead to the error conclusion that no violation has taken place, even where the enjoyment of fundamental rights has been significantly impaired.

A notable example can be seen in the treatment of large-scale distributed denial-of-service (DDoS) operations, such as those carried out during the 2007 cyberattacks on Estonia, which disrupted government, banking, and media services for days[83]. Despite the significant societal and economic impact, these operations were generally not classified by legal scholars as a "use of force" or "armed attack" under *jus ad bellum*, largely because they did not result in physical destruction or loss of life[84].

---

[82] Ibid, 465.
[83] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (NATO Cooperative Cyber Defence Centre of Excellence, 2010), p. 14-33. https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf
[84] Ibid, 14-33.

Digital technologies increasingly shape all aspects of human life, affecting not only direct users but also individuals indirectly through the actions of states, corporations, and other actors that develop, control, or benefit from these technologies. As the Internet has evolved into an essential environment for communication, such transformation raises a critical question: how should violations of human rights perpetrated within the digital sphere be identified, attributed, and addressed, particularly in a context where responsibility is diffused among multiple actors and the harm may not always produce immediate or visible consequences.

This problem becomes particularly evident in the context of cyber operations targeting critical infrastructure, where the disruption of essential services often causes serious human consequences without fitting neatly into traditional understandings of harm. This problem is aggravated by the structure of digital infrastructure. Critical systems such as power grids, water networks, and hospitals are deeply connected to one another, which means that when one is attacked, the effects spread far beyond the initial point of disruption. For example, the the WannaCry ransomware attack significantly disrupted hospital operations, including the UK National Health Service, leading to cancelled procedures and delays in patient care despite the absence of direct physical destruction[85]. The harm that follows, people losing access to medical care, unsafe living conditions, disruption of basic services, tends to build up slowly and affect large numbers of people over time, rather than striking in a single, obvious moment.[86]

But the idea is not to criticize the connection within the infrastructural system, rather to point out a problem that often gets overlooked: when cyber attacks are launched, most of the time, just the just the technical disruption is acknowledged. This is precisely why the violation error emerges: not because lawmakers and practitioners are unaware of the problem or unwilling to act, but because the law was designed

---

[85] Roger Collier, "NHS Ransomware Attack Spreads Worldwide," *CMAJ* 189, no. 22 (2017). https://pmc.ncbi.nlm.nih.gov/articles/PMC5461132/

[86] International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Building a Culture of Compliance for IHL to Protect Humanity in Today's and Future Conflicts* (2024): 37-40. https://www.icrc.org/en/publication/international-humanitarian-law-and-challenges-contemporary-armed-conflicts-building

around a different kind of harm. Traditional human rights frameworks expect a clear act, a responsible actor, and an identifiable victim: a shot in the leg – physical damage, a burnt building – destruction of property, a kidnapping – deprivation of freedom. The logic is simple and the harm is visible.

Cyber attacks on critical infrastructure rarely offer any of these in a straightforward way. The damage spreads through chains of system failures, the people affected may be far removed from the original target, and the consequences may take days or weeks to fully materialize. The result is that entire populations can be left without access to rights as basic as health, clean water, or an adequate standard of living, yet no formal violation is ever recorded, not because nothing happened, but because what happened does not fit the shape that the law recognizes as a violation. Understanding this gap and it affects the protection of human rights in the context of cyber attacks on critical infrastructure requires a deeper analysis of the nature of such attacks and their real examples.

2.2 Cyber attacks and critical infrastructure

There were and still are many proposed definitions of cyber attacks, and since the cyber world would not exist without technical specialists, the proposals come both from the legal, tech and cybersecurity communities. Those definitions include different elements and reflect the core interest of the community proposing them. For example, the definition can be as short as “any intentional attempt to disrupt or destroy another country’s computer networks” to broader “actions taken by countries to infiltrate the computers or computer networks of a country or other countries to cause damage or disruption”[87]. As of 2026, there is no universally accepted definition inside the legal community, just like there are multiple approaches to assessment of cyber operations under *jus ad bellum,* and the emergence of one remains unlikely. The lack of a unified definition is not exceptional. Article 8 of the European Convention on Human Rights

[87] Yuchong Li and Qinghui Liu, “A Comprehensive Review Study of Cyber-Attacks and Cyber Security: Emerging Trends and Recent Developments,” *Energy Reports* 7 (2021): 8177. https://www.sciencedirect.com/science/article/pii/S2352484721007289

and the European Court of Human Rights provide no exhaustive definition of "private life", relying instead on evolving interpretation[88]. Similarly, the notion of a cyber attack remains open to interpretation and shaped progressively through existing doctrine and practice, rather than inventing a newly constructed exhausting framework.

According to the Rule 92 of the Tallin Manual 2.0, a cyber attack, as it is outlined by the authors of the Manual, is destructive in nature. Non-violent attacks, that may cause some other non-kinetic harm, do not qualify as a cyber attack, even though the definition of "attack" according to the Article 49 of the Additional Protocol I to the Geneva Conventions (AP I) does not mention destruction or kinetic consequences[89]. Therefore, it all comes down to the agreed definitions and traditional international humanitarian law, since it was built around the concept of physical violence and material damage as a core threshold. The logic comes out of the different structuring of war crimes, where only certain offences are qualified as attacks under IHL[90] or ICL, while others, like pillage or destruction of property, do not[91]. This distinction demonstrates that not all hostile acts are intended to qualify as attacks, but rather that "attack" is a narrower legal concept linked to acts of violence, consistent with its traditional meaning under AP I[92]. So, it was logical for the authors of the Tallin Manual 2.0 to adapt their definition of cyber attack to the general understanding of attack without breaking the traditional IHL pattern. However, just like the cyber attacks are complex, the nature of cyber attack's consequences is complex, as well. As it was mentioned earlier, for traditional attacks the consequences are much more straightforward – a state launches a missile at an opposing army's command center, destroying it and sometimes even civil infrastructure, if due to the technical failure the strike misses the intended military objective. The destruction is direct and immediate,

---

[88] European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence*, p. 56-76. https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng

[89] Schmitt, Michael N., ed. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." 2nd ed. Cambridge: *Cambridge University Press*, (2017): 415 .

[90] ICRC, "Commentary on Article 33," in *Convention (IV) Relative to the Protection of Civilian Persons in Time of War of 12 August 1949: Commentary of 2025*. https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-33/commentary/2025.

[91] Chris Jenks, "Motive Matters: The Meaning of Attack Under IHL & the Rome Statute," *Opinio Juris*, 26 October 2020. http://opiniojuris.org/2020/10/26/motive-matters-the-meaning-of-attack-under-ihl-the-rome-statute/

[92] Ibid.

however, when that state launches a cyber attack. The consequences often can be illustrated by or imagined as falling dominos – a DDoS operation overwhelms the control systems of a power plant, causing it to fail and leaving parts of the country without electricity, with the consequences manifesting from the simple digital disruption to tangible failure of essential civilian infrastructure[93].

The nature of a cyber attack is closely interconnected with its phases, way before the consequences happen, whether direct or indirect, detailed planning happens behind the scenes. For instance, the Tallin Manual 2.0 recognizes that cyber attacks can involve multi-stage processes as some of them can even be a 'series of cyber operations' or 'composite acts', the legal assessment of them depends on their cumulative scale and effects rather than on isolated actions. Cyber attacks are often perceived in simplified terms, and for many people can be a mere use of malicious code, that is why some countries do not take it as serious as those that experienced such attacks[94]. For example, Lithuanian government took the 2008 cyber incidents, which involved DDoS attacks against government institutions and public websites following political tensions, temporarily disrupting access to state information systems, with much more seriousness than expected[95]. In contrast, comparable cyber operations in the United States, such as those surrounding the 2016 United States election interference, were primarily treated as issues of election security, while Obama described them "as a mere violation of established international norms of behavior."[96]

But in reality, they constitute complex, multi-layered operations that should not be underestimated or disregarded both in peaceful times and in warfare. Every cyber attack, regardless of its motive or the legal context in which it occurs – whether peacetime or armed conflict, starts with reconnaissance[97]. This first phase involves the research, identification, and selection of targets through the systematic aggregation of

---

[93] Eneken Tikk, Kadri Kaska, and Liis Vihul, "International Cyber Incidents: Legal Considerations", NATO Cooperative Cyber Defence Centre of Excellence, (2010): p. 81
[94] Ibid, 57.
[95] Ibid, 57.
[96] Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?," *Texas Law Review* 95 (2017): 1579.
[97] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research* 1 (2011): 4.

publicly accessible online information[98]. The second phase is weaponization during which tools are developed and assembled with the specific aim of compromising the identified target, at this point the attacker formulates a strategic approach, identifies vulnerabilities to be exploited, and develops malware designed to evade detection within the target system[99]. The delivery phase marks the point at which the cyber weapon is transmitted into the target environment. In a cyber warfare context, this may involve spear-phishing emails sent to employees of a power grid operator, compromised websites used to distribute malware to government officials, or infected removable media introduced into secure military systems[100]. Although no physical force is used at this stage, delivery represents a critical transition from preparation to execution, as it initiates the intrusion into systems that may constitute military objectives or civilian infrastructure under AP I. Once delivered, the exploitation phase triggers the malicious code by taking advantage of identified vulnerabilities[101].

In the context of cyber operations against critical infrastructure, exploitation is the stage at which the attack begins to materialize functionally, and while still not necessarily producing physical damage, this phase is crucial in enabling subsequent harmful effects. The installation phase ensures persistence within the targeted system, typically through the deployment of backdoors or remote access tools[102]. Following installation, the command and control (C2) phase establishes a communication channel between the attacker and the compromised system, effectively granting continuous operational control[103]. For example, attackers may remotely manipulate the functioning of a power grid or coordinate actions across multiple infected systems. At this stage, the operation becomes actively controllable, raising important legal questions

---

[98] Ibid, p. 4.
[99] Eva Rodríguez Vidal, "The Seven Phases of a Cyberattack: A Detailed Look at the Cyber Kill Chain," *Sngular Insights*, 26 March 2025. Accessed March 23, 2026. https://www.sngular.com/insights/360/the-seven-phases-of-a-cyberattack-a-detailed-look-at-the-cyber-kill-chain
[100] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research* 1 (2011): 4-8.
[101] Ibid, 4-8.
[102] Ibid, 5-8.
[103] Ibid, 5-8.

regarding attribution and the moment at which the conduct becomes sufficiently harmful to qualify as an "attack" under IHL.

Finally, the actions on objectives phase represents the culmination of the operation, where the attacker achieves their intended goal. In cyber warfare, this may include disrupting electricity supply, manipulating water treatment processes, or disabling military systems. Here, the consequences may manifest in tangible harm, such as loss of essential services or damage to infrastructure, thereby bringing the operation closer to the traditional understanding of an "attack" as an act of violence. Without understanding the technical aspects of cyber attacks, it is difficult to accurately access their nature and legal implications, not only within the theoretical framework of defining a cyber attack, but also in its practical application. Importantly, these phases illustrate that the nature of cyber attacks cannot be reduced to a single moment but must be understood as a sequence of interconnected actions whose legal qualification depends on their cumulative effects[104].

The cyber operations with the purpose of disrupting Ukrainian civilian infrastructure started a couple years before the full-scale invasion, with some scholars and military experts hypothesizing that the idea behind those attacks laid in the Russia's desire to "signal its capability and a willingness to expand its use of offensive cyber operations to achieve kinetic effects"[105]. Although, all of the described attacks will be considered as "allegedly" carried by Russian cyber forces and no official attribution exists in the strict sense of international law, the disclaimer should be made that there is strong evidence that the Kremlin has resourced or at least "ordered" such attacks. In fact, the pre-2022 attacks have already been blamed on Russia by Ukrainian authorities[106] and former NATO officials[107].

---

[104] Eneken Tikk, Kadri Kaska, and Liis Vihul, "International Cyber Incidents: Legal Considerations", NATO Cooperative Cyber Defence Centre of Excellence, (2010): 81.

[105] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare", CNA Occasional Paper DOP-2016-U-014231-1Rev, Center for Naval Analyses, (2017), p.19. https://apps.dtic.mil/sti/pdfs/AD1032208.pdf

[106] James Titcomb, "Ukrainian Blackout Blamed on Cyber-Attack in World First," *The Daily Telegraph*, 5 January 2016. https://www.telegraph.co.uk/technology/news/12082758/Ukrainian-blackout-blamed-on-cyber-attack-in-world-first.html?ICID=continue_without_subscribing_reg_first

[107] Sarah J. Lohmann et al., "*What Ukraine Taught NATO about Hybrid Warfare*", US Army War College Press (2022). https://press.armywarcollege.edu/monographs/956/

Among such evidence is the use of specific malware code, that is often used by different hackers of Russian nationality, overlapping tools or similar in design techniques that are used during the cyber operations, and other digital "fingerprints" that connect the hackers to Russia's military intelligence services, like files in Russian language and the usage of a Russia-based internet provider[108]. Moreover, Ukrainian Security Services are not the only ones trying to identify the hackers or prove their ties with the Kremlin. In 2020, a federal grand jury in Pittsburgh charged six Russian nationals with seven counts of various computer frauds and identity thefts, and those individuals were tied to the group that deployed multiple destructive malwares, including the 2015 BlackEnergy attack on Ukrainian infrastructure[109]. The American authorities also established that the hackers officers of the Unit 74455 of the Russian Main Intelligence Directorate (known as "GRU")[110]. It is also important to note that many cyber attacks were also carried out in other fields, some – to gain access to governmental institutions data, other – to infect media outlets, thus, the amount of cyber operations against Ukraine is much greater than it may seem based on the infrastructure sphere alone, with Community Emergency Response Team reporting over 15 thousand incidents in the last few years[111].

In 2015, Sandworm used a malware toolkit called BlackEnergy to begin a spear-phishing campaign against employees of Ukrainian power companies. Spear-phishing involves deceptive emails that are used to trick individuals and organizations into revealing sensitive information, and in this case the emails were impersonating the Ukrainian Minister of Industrial Policy and installing files that allowed hackers to monitor logins, activity patterns, steal credentials authentication data. This information

---

[108] Muzyka, V. V. "Analiz kiberatak proty system enerhozabezpechennia Ukrainy v konteksti konfliktu na Donbasi" [Analysis of Cyber-Attacks on Ukrainian Power Grid Systems in the Context of Armed Conflict in Donbas]. *Pravova Derzhava*, vyp. 39 (2020): 79

[109] US Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," press release, 19 October 2020. https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

[110] Ibid.

[111] "Critychna infrastruktura pid prytsilom: yak Ukraina vybudovuye kiberstiykist i choho svit mozhe v nas povchytys" ["Critical Infrastructure under Fire: How Ukraine Builds Cyber Resilience and What the World Can Learn"]. *Hromadske*, 2025. https://hromadske.ua/specials/254318-krytychna-infrastruktura-pid-prytsilom-iak-ukrayina-vybudovuye-kiberstiykist-i-choho-svit-moze-v-nas-povchytys

was used to move from the corporate network into operational systems, which then let Sandworm remotely access software used by control centers to manage operational control over the electrical grid[112]. At that time, the team has moved through almost all of the earlier described stages, from reconnaissance to command and control, but they strategically waited for the evening of December 23, 2015 and only launched the attack during the shift change. The last and most active phase of the attack involved direct manipulation of industrial control systems to disrupt electricity distribution, disable backup systems, and deploy destructive tools to delay recovery, which ultimately translated this digital intrusion into tangible physical consequences in the form of widespread power outages[113]. These outages affected nearly 225 thousand Ukrainians for a couple of hours[114], disrupting access to essential services that are closely linked to the protection of fundamental human rights, and this issue will be addressed more fully in the next subchapter. This was one of the first attacks that illustrated the hybrid nature of cyber operations, where digital intrusion equaled physical effects. Rather than relying on destructive malware to damage equipment, the attackers gained access to supervisory control and data systems and issued commands to disrupt electricity supply. This distinguishes such operation from traditional conceptions of attack grounded in physical destruction, as the effects were primarily operational and reversible, with power restored within several hours. However, the temporary character of the disruption does not diminish its significance, it proves completely opposite thing, the coordinated and multi-layered execution, including the disabling of backup systems making it impossible for the Ukrainian power grid workers to stop or control the attack, demonstrates a high degree of planning and control over critical infrastructure. Therefore, this case study illustrates that cyber operations can possess a distinctly military character and high preparation even in the absence of “traditional” physical

[112] Miles Pollard, “A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States,” *Pepperdine Policy Review* 16, no. 1 (2024): 6-15.
[113] MITRE ATT&CK. "2015 Ukraine Electric Power Attack." Campaign C0028. 2024. https://attack.mitre.org/campaigns/C0028/
[114] Samuele De Tomas Colatin, "Power Grid Cyberattack in Ukraine (2015)," *International Cyber Law: Interactive Toolkit*. NATO Cooperative Cyber Defence Centre of Excellence. https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015)

damage, what challenges simply effect-based interpretations of the use of force and supports a broader, character-based understanding of cyber warfare.

In 2016, a similar cyber operation was carried out, allegedly, by the same hackers group Sandworm, but with the usage of a much more sophisticated malware – Industroyer. In comparison to the previous attack, it had only power systems in some districts of Kyiv and lasted barely more than an hour[115]. However, cyber threat specialists note that, based on the files and the malware design, the intended scale of the attack was far larger and was significantly different from what the hackers achieved[116]. Even though the private and state investigations were carried out, the absence of an international body able to determine attribution and make authoritative findings also contributed to international uncertainty[117]. And in the April of 2022, two months after the start of the full-scale invasion, The Ukrainian Government Computer Emergency Response Team undertook urgent response measures following an information security incident involving a targeted cyber attack against a Ukrainian energy facility, and prevented the Industroyer2 attack[118]. The attackers' plan, again, aimed to disrupt multiple critical components of the targeted infrastructure. And at that point, the cyber attacks have been expected due to the Ukrainian Main Directorate of Intelligence, which highlighted the preparation of GRU's hackers for the intense DDoS attacks on Ukrainian critical infrastructure, as well as Ukraine's closest allies[119]. A much less documented example of a cyber attack is the FrostyGoop attack on Lviv's critical infrastructure. Sa security experts point out, FrostyGoop is oone of the few malwares, which intended purpose was physical damage, instead of just stealing data[120].

---

[115] Muzyka, V. V. "Analiz kiberatak proty system enerhozabezpechennia Ukrainy v konteksti konfliktu na Donbasi" [Analysis of Cyber-Attacks on Ukrainian Power Grid Systems in the Context of Armed Conflict in Donbas]. *Pravova Derzhava*, vyp. 39 (2020): 79.

[116] Joe Slowik, "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack", Dragos, Inc (2019): 3. https://pylos.co/wp-content/uploads/2021/02/crashoverride.pdf p3

[117] Muzyka, V. V. "Analiz kiberatak proty system enerhozabezpechennia Ukrainy v konteksti konfliktu na Donbasi" [Analysis of Cyber-Attacks on Ukrainian Power Grid Systems in the Context of Armed Conflict in Donbas]. *Pravova Derzhava*, vyp. 39 (2020): 79.

[118] CERT-UA, "Cyberattack by Sandworm Group (UAC-0082) on Energy Facilities of Ukraine Using Malicious Programs INDUSTROYER2 and CADDYWIPER," CERT-UA#4435, 12 April 2022. https://cert.gov.ua/article/39518

[119] Defence Intelligence of Ukraine, "Invaders Preparing Mass Cyberattacks on Facilities of Critical Infrastructure of Ukraine and Its Allies," 26 September 2022. https://gur.gov.ua/en/content/okupanty-hotuiut-masovani-kiberataky-na-obiekty-krytychnoi-infrastruktury-ukrainy-ta-ii-soiuznykiv.html

[120] "Modbus Vulnerabilities Used for Cyberattack on a Heating Utility," *Veridify Security*, 26 July 2024. https://www.veridify.com/article/modbus-vulnerabilities-used-for-cyberattack-on-a-heating-utility/

It was also one of the attacks that caused the collapse of Ukrainian infrastructure, mainly the districting heating, in one of the largest cities – Lviv. More than 100 thousand people in over 600 buildings in the district of Sykhiv had no heat and no hot water for 48 hours in a cold January weather[121], and, unfortunately, due to the Russian missile attacks in winter of 2026, even more people experienced such this. American cybersecurity experts found that the communication protocol of the heating control system was connected to Moscow-based IP addresses, with some of them suggesting that the cyber attack on heating infrastructure in the middle of winter may reflect a shift toward more intensive cyber sabotage, particularly in western regions of Ukraine, as Russia's missile strikes become less effective due to improved Ukrainian air defense[122].

From a legal perspective all the described above operations highlight the growing inadequacy of purely effects-based approaches in assessing cyber activities under international law. Even in the absence of massive physical destruction, operations directed at critical infrastructure, especially those capable of disabling essential services or undermining system integrity, challenge the traditional distinction between mere interference and a prohibited use of force under Article 2(4) of the UN Charter. At the same time, this challenge is not entirely unaddressed within existing legal frameworks. The practice of the International Criminal Court demonstrates an increasing willingness to move beyond a strictly incident-based assessment by taking into account the cumulative effects of multiple acts and their broader impact over time. In this sense, even operations that may appear limited when viewed in isolation can contribute to a pattern of conduct that produces significant harm[123]. These cases practically support the view that the legal qualification of cyber operations should not depend simply on immediate, observable damage, but must also account for the nature, intent, and functional impact of the operation, including its capacity to generate

[121] Ibid.

[122] "Novyi vyd rosiiskoho teroryzmu: moskovski khakery navchylys' vidkliuchaty opalennia v budynkakh, pochavshy zi Lvova – rozvidka Wired" [A New Form of Russian Terrorism: Moscow Hackers Learned to Shut Off Heating in Buildings, Starting with Lviv – Wired Investigation]. Forbes Ukraine, 24 July 2024. https://forbes.ua/war-in-ukraine/noviy-vid-rosiyskogo-terorizmu-moskovski-khakeri-navchilisya-vidklyuchati-opalennya-v-budinkakh-pochavshi-zi-lvova-rozvidka-wired-24072024-22598.

[123] ICC Office of the Prosecutor, *Policy on Cyber-Enabled Crimes under the Rome Statute* (ICC, December 2025), para. 99. https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf

cascading or delayed harmful effects. In this context, such operations illustrate the need for a more nuanced legal framework that captures the systemic and potentially destructive character of cyber activities, even where their consequences do not neatly align with traditional kinetic destructive consequences. Importantly, the FrostyGoop incident underscores that harm in cyberspace is not always immediately perceptible. Even where essential services are not fully disabled, the compromise of technical system integrity may generate significant societal risks. These risks translate into indirect, yet very real, implications for the enjoyment of fundamental human rights, including access to basic services and personal security.

This broader understanding can be seen also through cyber operations targeting sectors such as telecommunications and banking, which may not traditionally be classified as "critical infrastructure" but nonetheless play an essential role in sustaining civilian life. Disruptions to networks such as Kyivstar or financial systems can significantly impair access to healthcare, limit the ability to pay for essential goods and services, and effect communication during armed conflict[124]. Moreover, these harms often manifest cumulatively, where multiple disruptions, whether to energy, communications, or financial systems, interact to produce severe humanitarian consequences. This supports a more integrated legal assessment in which cyber operations are evaluated not in isolation, but in light of their combined impact on civilian life and dignity, consistent with evolving interpretations of international humanitarian law and international criminal law.

Having examined how cyber operations target and disrupt critical infrastructure, it becomes evident that their significance extends beyond technical interference or strategic advantage. These incidents must also be understood through the lens of their human consequences, as disruptions to essential services directly affect the enjoyment of fundamental rights. This shift in perspective is particularly important from a legal standpoint. Traditional analyses of cyber operations often prioritize questions of attribution, use of force, and state responsibility, yet risk underemphasizing the lived

[124] Evans Mugari, "Kyivstar Cyber Attack: A Deep Dive into Cyber Warfare in Ukraine," *SIGNAL Media* (AFCEA International), July 2025. https://www.afcea.org/signal-media/cyber-edge/kyivstar-cyber-attack-deep-dive-cyber-warfare-ukraine

impact of such operations on civilian populations. By focusing on infrastructure, cyber attacks indirectly but profoundly interfere with access to electricity, water, healthcare, and communication systems, services that are closely intertwined with the effective enjoyment of fundamental human rights. As such, the consequences of cyber operations cannot be truly and deeply assessed without situating them within a human rights framework.

2.3 The human rights dimensions of cyber attacks on infrastructure: expanding the scope of harm

As Assistant Attorney General for National Security for the United States, John C. Demers, noted on the day of the earlier 2020 indictment concerning Russian state-linked hackers of the GRU Unit 74455, "No country has weaponized its cyber capabilities as maliciously or irresponsibly as Russia, wantonly causing unprecedented damage to pursue small tactical advantages and to satisfy fits of spite"[125]. It is difficult to disagree with such a statement, however, when covering such cyber operations, the news tend to prioritize the political and strategic dimensions of such attacks, while devoting comparatively limited attention to their human rights implications. This asymmetry in focus shows that their impact on fundamental rights and civilian well-being remains underexplored. This is also understandable, as was described in the violation error subchapter, less direct and non-kinetic aftermath of cyber attacks, and in some cases, traditional attacks, get less attention, however, the lack of destruction should not amount to the lack of responsibility. In fact, there is also space to argue that all of the earlier mentioned attacks did lead to, if not complete destruction, but to the violation of human rights and should not be ignored in terms of international responsibility, whether in connection or outside of the armed conflict.

[125] United States Department of Justice. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." Press release. 19 October 2020. https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

Critical infrastructure comprises systems and functions essential to the uninterrupted functioning of society, including energy grids, transport networks, and water supply systems. Cyber attacks targeting these systems, as it has been described, have become increasingly frequent, sophisticated, and precise, which enables attackers to disrupt or damage physical infrastructure by infiltrating the digital systems that control critical processes, often with different societal and environmental consequences. Some scholars correctly point out that while the technical side of cybersecurity threats and attacks have be extensively researched, not many academic sources analyze the human rights and societal dimensions of them[126].

At the most fundamental level cyber attacks can pose a risk to the right to life through disrupting energy systems, water supply or transportation. Article 6 of the International Covenant on Civil and Political Rights (ICCPR) states that "no one should be arbitrarily deprived of his life"[127]. Despite its laconic wording, the provision carries a deeper message that is connected to the consequences of cyber attacks, including the earlier mentioned ones. In its commentary to the Article 6, the Human Rights Committee interprets the right to life and its protection while including essential goods and services such as electricity, water, healthcare and recognizes that cyber attacks can disrupt such essential to the life services[128]. This interpretation reinforces the right to life and its protection as extending beyond mere protection against arbitrary killing and highlights that the understanding that the right to life is not limited to immediate physical harm but also includes protection against reasonably foreseeable threats arising from the disruption of critical infrastructure, particularly where such interference may impair emergency response systems or deprive individuals of basic conditions necessary for survival[129].

---

[126] Johan Ninan, Bharadwaj R. K. Mantha, and Balaji Kesavan, "Human-Centred Cybersecurity for Critical Infrastructure: The Case of the Florida Water Plant Hack," *Engineering, Construction and Architectural Management* 32, no. 13 (2025): 547.

[127] International Covenant on Civil and Political Rights. Adopted 16 December 1966. Entered into force 23 March 1976. 999 UNTS 171.https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[128] Human Rights Committee, *General Comment No. 36: Article 6 (Right to Life)*, UN Doc. CCPR/C/GC/36 (3 September 2019). https://documents.un.org/doc/undoc/gen/g19/261/15/pdf/g1926115.pdf

[129] Ibid.

Closely connected is the right to health under the International Covenant on Economic, Social and Cultural Rights (ICESCR), as, for example, cyber operations that target power grids and cut off the electricity, just like dominos, affect healthcare systems, hospital databases, and pharmaceutical supply chains, which then interrupt access to treatment, undermining both availability and quality of care. The UN Committee on Economic, Social and Cultural Rights while commenting on the interpretation of the right to heath, included availability, accessibility, acceptability, and quality of healthcare services as parts of it[130], therefore, it can be added to the list of rights that are at the risk of being violated or, at the very least, affected by the consequences of a cyber attack.

The right to education and the right to work become increasingly vulnerable when cyber attacks lead to the disruption of electricity, especially considering that many kids and adults are still studying or working online. Cyber attacks on energy grids or water systems can also severely affect the right to an adequate standard of housing and living, as recognized in ICESCR. Under Article 11, the right to an adequate standard of living also includes access to essential services such as safe drinking water, sanitation, and energy for heating and basic domestic needs, all of which are considered are important in ensuring human dignity and survival[131]. Prolonged outages deprive individuals of adequate services that are a part of housing, thereby degrading living conditions. The European Court of Human Rights, in it's jurisprudence, for example, in *M. S. S. v. Belgium*, emphasizes that living conditions that lack basic services or even pose a risk to life due to the lack of access to sanitation or infrastructure failure can amount to degrading treatment[132]. It follows that comparable consequences should likewise be taken into account within the frameworks

---

[130] Committee on Economic, Social and Cultural Rights, *General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12)*, UN Doc. E/C.12/2000/4 (11 August 2000). https://www.ohchr.org/sites/default/files/Documents/Issues/Women/WRGS/Health/GC14.pdf

[131] Committee on Economic, Social and Cultural Rights, *General Comment No. 4: The Right to Adequate Housing (Art. 11(1) of the Covenant)*, UN Doc. E/1992/23 (13 December 1991). https://www.refworld.org/legal/general/cescr/1991/53157

[132] *M.S.S. v. Belgium and Greece* [GC], App. No. 30696/09 (ECtHR, 21 January 2011), para.362-368., 2026. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-103050%22]}

of international criminal law and international humanitarian law when assessing the legality and human impact of actions affecting civilian populations.

At a general level, IHL protects civilians and civilian objects through its foundational principles of distinction, proportionality, and precautions in attack, codified in multiple legal instruments, such as the Geneva Conventions and Additional Protocol I. The principle of distinction obliges parties to an armed conflict to distinguish at all times between civilians and combatants, as well as between civilian and military objects. The principle of proportionality prohibits attacks expected to cause incidental civilian harm excessive in relation to the concrete and direct military advantage anticipated, thereby embedding a balancing mechanism that implicitly acknowledges the value of civilian life and well-being. The obligation to take precautions further requires attackers to minimize incidental harm, including by choosing means and methods of warfare that reduce risks to civilians.

Under IHL, the protection of life is operationalized through prohibitions on targeting civilians and rules governing the conduct of hostilities. The killing of civilians is not per se unlawful if it occurs as incidental harm in a lawful attack that complies with proportionality and precaution requirements. Article 54 of AP I, for instance, prohibits the starvation of civilians as a method of warfare and forbids attacks against objects such as foodstuffs, agricultural areas, drinking water installations, and irrigation works[133]. Similarly, Article 56 provides special protection for works and installations containing dangerous forces, such as dams and nuclear power plants, recognizing the severe humanitarian consequences that their destruction may entail[134]. These provisions reflect an implicit acknowledgment of the importance of maintaining basic living conditions, even if framed in terms of prohibitions on specific conduct rather than positive rights. The jurisprudence of international criminal tribunals, including the ICTY, and many academic sources, has further elaborated on these protections, particularly in cases involving the targeting of civilian infrastructure and

[133] *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts*, art. 54. https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-54
[134] *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts*, art. 56. https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-56

the use of siege tactics that deprive populations of essential resources. As noted in the Tallinn Manual 2.0 comments, the application of IHL to contemporary forms of warfare, including cyber operations, raises complex questions about how non-kinetic effects should be assessed under these principles, particularly when the harm manifests through disruption of essential services rather than immediate physical destruction[135].

Therefore, it is logical to assume and advocate for the interpretation that cyber operations which intentionally disable or significantly disrupt access to indispensable civilian service, like electricity, water supply, heating, or sanitation, should fall within the legal concept of "attacks" under IHL, even in the absence of kinetic damage[136]. And as it was mentioned before, the restrictive reading of "attack" as requiring material damage risks creating a normative gap whereby operations capable of endangering civilian life and dignity evade legal scrutiny, thereby undermining the protective purpose of IHL.

This interaction becomes particularly important when considering the relationship between international humanitarian law and international human rights law. While IHL regulates the conduct of hostilities through rules on targeting and proportionality, the ICCPR, particularly Article 6, as interpreted by the UN Human Rights Committee in General Comment No. 36, establishes a broader obligation to protect the right to life, including against reasonably foreseeable threats arising from the deprivation of essential services. The Human Rights Committee explicitly recognizes that states must take positive measures to ensure access to basic necessities such as food, water, and healthcare, thereby extending the protection of life beyond direct violence to conditions that may threaten survival[137]. In this sense, IHL and international human rights law operate in a complementary manner: while IHL sets limits on conduct during armed conflict, human rights law reinforces the need to assess

[135] Schmitt, Michael N., ed. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd ed. Cambridge: *Cambridge University Press* (2017): 415 .
[136] Kubo Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law," *Israel Law Review* 48, no. 1 (2015): 56.
[137] Human Rights Committee, *General Comment No. 36: Article 6 (Right to Life)*, UN Doc. CCPR/C/GC/36 (3 September 2019), para. 26–30. https://www.ohchr.org/en/calls-for-input/general-comment-no-36-article-6-right-life

the broader humanitarian consequences of operations, including those that impair access to indispensable infrastructure.

This interpretation seems to be consistent with the object and purpose of the Geneva Conventions and their Additional Protocol I, which aim to limit the effects of armed conflict on civilians and civilian objects. The definition of attacks in Article 49 of AP I refers to "acts of violence against the adversary," a formulation that does not explicitly require physical destruction but rather emphasizes the harmful nature of the act[138]. Therefore, this provision suggests that "violence" may encompass not only kinetic force but also operations that foreseeably produce severe harm through the disruption of essential systems. In the ICRC Commentary to AP I, this notion of "violence" was primarily understood in the context of traditional, kinetic forms of warfare, reflecting the technological realities of the time. However, more recent ICRC Commentaries and reports demonstrate an evolution in interpretation, acknowledging that contemporary means and methods of warfare may produce harmful effects without the use of physical force. In particular, the ICRC's work on new technologies in warfare emphasize that the application of IHL must remain responsive to developments such as cyber operations, focusing on their consequences for civilians rather than the specific means employed[139].

In this regard, cyber operations targeting power grids, water treatment facilities, or hospital networks, thereby depriving civilian populations of vital services, can be understood as functionally equivalent to attacks on those objects, given that the resulting humanitarian consequences, including risks to life, health, and basic living conditions, are both foreseeable and, it would be foolish to disagree that, in many cases, intended.

Additionally, this broader interpretation aligns with the principle of distinction, which protects civilian objects unless and for such time as they become military objectives. While some critical infrastructure may qualify as dual-use, because military

---

[138] *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts*, art. 49. https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-49?activeTab=

[139] ICRC, "*International Humanitarian Law and Cyber Operations during Armed Conflicts"*, ICRC Position Paper (ICRC, November 2019), p.4-7. Accessed April 5, 2026 https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf

object still needs electricity and water and are often connected to the same systems as civilian buildings, even if there is a military advantage, attackers still must consider all the possible harm their actions could cause to civilians. As emphasized by the ICRC, the assessment of proportionality must include reverberating and cascading effects. In the Commentary on the proportionality ICRC directly states that "a cyber operation could incidentally disable civilian objects without physically damaging them; but the effects may be more widespread due to the interconnectedness of cyberspace"[140] thus highlighting that even such non-kinetic aftermath should be taken into the account under the IHL. Ignoring such effects of cyber attacks would artificially narrow the scope of legal protection and fail to capture the realities of modern, interconnected societies.

As was affirmed by the ICJ, international humanitarian law and international human rights law operate concurrently, and their norms should be interpreted harmoniously where possible[141]. From this perspective, prolonged deprivation of electricity or water, particularly in extreme conditions, may engage the right to life, the right to health, and the right to an adequate standard of living, as protected under the ICCPR and the ICESCR, should also be taken into the account when the analysis of the attack is done through the IHL lens. When such deprivation is the foreseeable result of a cyber operation conducted in the context of an armed conflict, it becomes increasingly difficult to justify its exclusion from the regulatory framework of IHL simply on the basis that no physical destruction occurred. Accordingly, recognizing disruptive cyber operations as "attacks" would not constitute a departure from existing law but rather an evolution in its interpretation, ensuring that its protective function remains effective in light of technological developments. It could also allow the legal community to close a critical accountability gap, ensuring that actors cannot circumvent legal obligations by relying on non-kinetic means that nonetheless produce

[140] International Committee of the Red Cross. "Cyber Operations during Armed Conflict: The Principle of Proportionality." Fact sheet. Geneva: ICRC, March 2023. https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/04_proportionality-0.pdf

[141] International Court of Justice. *Legality of the Threat or Use of Nuclear Weapons*. Advisory Opinion. I.C.J. Reports 1996, p. 226. 8 July 1996. https://iilj.org/wp-content/uploads/2016/08/Legality-of-the-Threat-or-Use-of-Nuclear-Weapons-1996.pdf

severe humanitarian consequences. In this sense, the qualification of such operations as attacks under IHL is not only just theoretic but a practically necessary to save the integrity of the law governing armed conflict and to ensure that its fundamental objective, the protection of human dignity, remains relevant despite new forms of warfare.

The preference of the legal community, including the authors of the Tallin Manual, for the effects-based approach and its simplicity comes at a significant conceptual cost. By privileging effects that mirror kinetic destruction of the "traditional" attacks that the international humanitarian law is used to, this approach risks excluding a wide range of cyber operations that are capable of producing severe harm through non-physical means, including ones described earlier. Those disruptions of critical infrastructure and interference with essential services did not result in immediate physical damage, yet their consequences, were equally impactful. More importantly, the reliance on observable effects does not resolve the underlying problem of attribution, rather, it shifts the analytical focus away from it. The difficulty of identifying the perpetrator remains, regardless of whether the operation caused physical destruction or functional disruption. In simple terms, the effects-based approach doesn't actually make things less complicated (because if it did, the global community might have already seen more cyber related accountability and more legal development in the sphere, than there is now), it avoids dealing with the difficult parts. By focusing only on visible outcomes (physical damage), it ignores important aspects of cyber operations, such as how they are carried out or what they are designed to do. Because of this, it may fail to fully reflect what cyber operations really are and how harmful they can be. This concern has been widely recognized in the literature, as well. For instance, Tsagourias notes that focusing on consequences alone does not resolve the attribution problem and risks oversimplifying the legal assessment of cyber operations, which are inherently complex and often deliberately obfuscated [142]. Similarly, Mačák emphasizes that an exclusive reliance on observable, kinetic-like

[142] Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution," *Journal of Conflict and Security Law* 17, no. 2 (2012): 232-240.

effects may fail to capture the distinctive nature of cyber operations, including their capacity to produce systemic and non-physical harm[143]. At the same time, these critiques do not suggest abandoning an effects-based or human-centric perspective altogether. On the contrary, scholars stress that the consequences of cyber operations, particularly their impact on individuals and access to essential services, remain central to legal analysis. As reflected in the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations and supported by open-access commentary, a more appropriate approach is to complement the assessment of effects with additional factors such as intent, context, and the cumulative impact of operations[144].

So, from a legal point of view, it is problematic to choose what is easier to analyze instead of what more accurately reflects the law and considers all aspect of it, combining international human right law, international humanitarian law and international criminal law. The characteristics of cyberspace, like anonymity, deniability, and technical opacity, exist independently of the legal frameworks designed to regulate it. Ignoring these characteristics, or trying to fit them into rules made for traditional warfare does not make their impact disappear. Instead, it just creates gaps in regulation and accountability. As the International Court of Justice has repeatedly emphasized in its jurisprudence, the interpretation of international law must evolve in light of changing factual circumstances, ensuring that its principles remain effective and relevant[145]. Applying this reasoning to cyber operations suggests that the legal community must engage directly with the complexities of cyberspace, rather than avoiding them through simpler analytical/theoretical models.

Ultimately, the choice between effects-based and nature-based approaches when it comes to analysing the results and objectives of the cyber attack in connection with the international human rights law, is not purely technical, but also normative, as it reflects broader assumptions about the purpose and adaptability of the legal system.

---

[143] Kubo Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law," *Israel Law Review* 48, no. 1 (2015): 56-59.

[144] Schmitt, Michael N., ed. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations". 2nd ed. Cambridge: *Cambridge University Press*, (2017): 415 .

[145] *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970)*, Advisory Opinion, I.C.J. Reports 1971, p. 16, para. 53 https://www.icj-cij.org/case/53

Prioritizing simplicity in the face of complexity risks making the law outdated, or at least insufficiently responsive to new forms of harm. By contrast, engaging with the inherent challenges of cyberspace, rather than avoiding them, allows for the development of a more robust and realistic legal framework, one that can account not only for the visible consequences of cyber operations but also for their underlying character and intent.In this sense, the task before the legal community is not to force cyber operations into existing categories, but to ensure that the categories themselves evolve in a manner that remains both true to the fundamental objectives of international law, such as the maintenance of peace, the protection of human dignity, and the accountability of those who violate these principles, and to the uniqueness of cyber space.

Some tech specialists, as was mentioned in the previous subchapter, note that based on the analysis of the malware code it is possible to determine that the cyber operation was designed to produce more severe damage than actually happened. However, simply because of technical malfunction or cybersecurity defenses, the malware may fail to produce its intended effects. This discrepancy between intended and realized harm also raises the same legal question: whether the qualification of such operations under International Humanitarian Law should depend exclusively on the outcome, or whether the design, intent, and inherent capability of the operation should also be taken into account.

In this context, a useful comparative analogy may be drawn from the concept of criminal attempt (“замах”) in Ukrainian criminal law, which recognizes that liability may arise even in the absence of a completed harmful result, provided that the perpetrator has undertaken substantial steps toward its realization. The idea is that the law is not only meant to react to harm that has already occurred, but also to address actions that create a real and immediate risk to protected interests. Applied to cyber operations, this means that the lack of immediate physical damage should not prevent legal qualification where an operation is intended to disrupt critical infrastructure or interfere with essential services. Just like an attempted crime, such cyber activities may fail to produce their full intended effects due to technical interruption or defensive

measures, however, their inherently harmful character and the risk they pose to civilian populations remain legally significant.

It is important to emphasize that this analogy does not suggest a direct transplantation of domestic criminal law concepts into international humanitarian law, but serves as an interpretative illustration supporting a broader point: that legal systems, across different fields, often recognize the necessity of addressing dangerous conduct before its most severe consequences materialize, or, in some cases, even if they do not materialize at all. In the cyber context, where operations may be capable of producing delayed or cascading effects, a strict focus on observable destruction as a threshold for legal qualification risks allowing harmful behavior to evade regulation. So, incorporating a more conduct-oriented perspective, similar in logic to the doctrine of attempt, may enhance the capacity of international law to respond effectively to the realities of contemporary warfare.

Overall, the choice between an effects-based and a more nature- or conduct-oriented approach is not merely a theoretical issue, but one that has direct implications for accountability. If only those cyber operations that result in visible, physical destruction are recognized within the scope of IHL, a significant range of harmful conduct, especially operations causing serious disruptions to essential services, fall outside legal qualification. This, in turn, risks creating gaps in responsibility, where actors engaging in potentially dangerous or even life-threatening cyber activities evade scrutiny simply because their actions did not produce immediate kinetic outcomes. For this reason, the way in which cyber operations are conceptualized at the level of IHL inevitably shapes how, and whether, they can be addressed within ICL, which will be explored in the next chapter.

***

The relationship between cyber operations and human rights protection reveals a fundamental problem: traditional legal frameworks struggle to capture the nature and consequences of attacks in the digital environment. Regardless of doctrinal approach, a persistent issue remains, which can be termed "violation error." Violation errors arise when significant interferences with human rights occur through digital means but are

not formally recognized as violations, often because their consequences are perceived as insufficiently severe. The absence of immediate or visible damage frequently leads to the mistaken conclusion that no violation has occurred, even where the effective enjoyment of fundamental rights has been impacted.

When multiple violations occur simultaneously, those that are more visible or physically destructive naturally receive greater legal and public attention, while less direct interferences risk being overlooked. However, such prioritization should not diminish the significance of harms that unfold gradually or through disruption of underlying infrastructure. These may affect a far broader population and undermine rights in a more pervasive manner. The concept of violation itself requires reconsideration: it should not be confined to moments of observable breakdown but should encompass processes that gradually erode access to essential services necessary for the realization of rights. Failing to acknowledge these less tangible harms risks normalizing legally invisible violations and weakening both accountability and the protective function of human rights law.

The absence of a universally accepted definition of cyber attacks reflects the open-textured nature of legal concepts rather than a fundamental deficiency. However, prevailing interpretations, particularly those aligned with the Tallinn Manual, remain narrowly focused on physical destruction, excluding non-kinetic operations capable of producing significant harm. Cyber attacks are not single acts but multi-stage cumulative processes: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and execution. Harm is embedded throughout the operation, not only at the final stage. Legal assessment focused solely on visible consequences ignores this composite nature.

Case studies from Ukraine illustrate this clearly. The 2015 power grid attack demonstrated how digital intrusion can produce physical consequences without destroying infrastructure, leaving approximately 225,000 people without electricity. The 2016 Industroyer attack and the attempted Industroyer2 operation in 2022 confirmed the increasing sophistication of such operations. The FrostyGoop incident in Lviv established an even more direct link between cyber interference and human

conditions, with disruption of heating systems leaving over 100,000 people without heat during winter. These examples show that cyber operations produce real-world harm through functional disruption even when systems remain physically intact, challenging effects-based approaches under international law, including interpretations of the use of force under Article 2(4) of the UN Charter.

The core issue is the continued reliance on visibility and physical damage as thresholds for legal qualification. A more adequate framework requires shifting toward a character-based approach that considers the intent, design, and operational capacity of cyber activities to disrupt critical infrastructure. It also requires incorporating indirect and cascading effects into proportionality analysis and recognizing that harm to infrastructure-dependent services constitutes legally relevant harm even without destruction.

Cyber attacks on critical infrastructure directly interfere with systems essential to human survival, like electricity, water, healthcare, and communications. Such disruptions engage rights protected under both the ICCPR and ICESCR, including the rights to life, health, education, work, and an adequate standard of living. These rights extend beyond protection against direct physical harm to foreseeable threats arising from the disruption of essential services.

International humanitarian law already contains principles capable of addressing such harm. The rules of distinction, proportionality, and precautions, as well as protections for objects indispensable to civilian survival, implicitly recognize the importance of maintaining essential living conditions. However, their interpretation remains constrained by a narrow understanding of "attack" tied to physical destruction. A broader interpretation grounded in Article 49 of AP I allows for the inclusion of operations that foreseeably cause harm through functional disruption, even without kinetic damage. This aligns with the object and purpose of IHL and ensures its protective function remains effective in technologically advanced contexts.

The reliance on an effects-based approach prioritizes analytical simplicity over accuracy. A shift toward a nature-based and conduct-oriented framework enables more precise assessment by incorporating intent, design, and capacity to produce harm,

including situations where operations are intended to cause significant disruption but fail due to technical factors, analogous to the concept of attempt in criminal law.

Without such adjustments, a significant category of harmful cyber activities remains insufficiently regulated, allowing serious interferences with civilian life to evade legal qualification and accountability.

CHAPTER 3

INTERNATIONAL CRIMINAL LAW AND CYBER CRIMES

3.1 Limits of international criminal law in ensuring individual accountability for crimes committed in cyber space

3.1.1 Limits within the Rome Statute

The mentioned characteristics of cyber operations – anonymity, non-kinetic nature, no clear operational boundaries and others – complicate questions of accountability, both state and individual. In traditional kinetic warfare, physical destruction and more easily identifiable perpetrators provide a clearer basis for legal accountability. In contrast, cyber operations often cause indirect or delayed harm, making it harder to prove causation, intent, and the level of seriousness needed for individual criminal responsibility[146]. As highlighted in Chapter 1, attribution and differences in approaches to cyber operations' consequences remain problematic in the context of state responsibility. However, the challenges established in relation to state responsibility become even more evident for individual criminal responsibility.

Although the ICC Office of the Prosecutor (OTP) has recently developed a Policy to address cyber-enabled crimes (OTP Policy on CEC)[147], significant limitations remain in the ability of international criminal law to ensure effective individual accountability for cybercrimes, both perpetrated in peacetime and armed conflict.

The first limitation lies in the lack of consensus regarding the core terms and concepts such as "cybercrime"[148]. Without a clear understanding of what conduct constitutes a cybercrime, and which specific characteristics distinguish such conduct from other, it is difficult to establish a basis for legal accountability. As noted in the

---

[146] Marco Roscini. "Gravity in the Statute of the International Criminal Court and Cyber Conduct That Constitutes, Instigates or Facilitates International Crimes", *30 Criminal Law Forum (*2019): 247-272.

[147] International Criminal Court, Office of the Prosecutor. "Questions and Answers: The ICC Office of the Prosecutor's Policy on Cyber-Enabled Crimes under the Rome Statute." 3 December 2025. https://www.icc-cpi.int/about/otp/questions-and-answers-the-icc-office-of-the-prosecutors-policy-on-cyber-enabled-crimes-under-the-rome-statute

[148] Kai Ambos. "International Criminal Responsibility in Cyberspace". *Research Handbook on Cyberspace and International Law* (2015): 118-143..

Tallinn Manual, the legal characterization of cyber conduct is a necessary pre-condition for determining the applicable legal framework and establishing responsibility[149]. However simply calling a conduct "cybercrime" (or whatever the consensus on the term may be) does not automatically make it legal or illegal, the characteristics of that conduct, like how and who carried it out and which effects it had matter as well. Cybercrime alone as a concept encompasses a wide variety of conducts, the Budapest Convention on Cybercrime lists data interference, computer-related forgery, offences related to child pornography, copyrights violations among other[150]. Therefore, when approaching the establishment of criminal accountability, there are two pathways that can be taken: limiting the scope of which conducts the term will include or expanding it so that the terminology itself can more clearly reflect the key elements and distinguishing characteristics of the conduct it designed to regulate. The Explanatory Report to the Budapest Convention on Cybercrime highlights that, at least in the authors' understanding, cybercrime covers both offences against computer systems (such as illegal access, data interference, and system interference) and offences committed by means of computer systems (such as fraud, child sexual abuse material offences, and copyright infringements), therefore, it must be an umbrella concept rather than a single offence category[151].

But not all scholars agree: some propose the use of a narrower term "computer network attacks" in relation to criminal accountability, which meaning can be still open to discussion, but it nevertheless has much more limited elements[152]. These elements include: no financial gain, purpose other than information gathering (as it is a core

---

[149] Schmitt, Michael N., ed. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd ed. Cambridge: *Cambridge University Press*, 2017.. https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017_.pdf

[150] *Convention on Cybercrime*. Opened for signature 23 November 2001. Entered into force 1 July 2004. European Treaty Series No. 185. Council of Europe. https://rm.coe.int/1680081561

[151] Council of Europe. *Explanatory Report to the Convention on Cybercrime*. European Treaty Series No. 185. Budapest, 23 November 2001. https://rm.coe.int/16800cce5b

[152] Kai Ambos. International Criminal Responsibility in Cyberspace. N. Tsagourias and R. Buchan (eds.), *Research Handbook on Cyberspace and International Law* (2015):118-143.

element of cyber espionage, which is excluded from computer network attacks), altering, destroying or disrupting a computer network or/and devices connected to it[153].

There have also been both legal and cybersecurity scholars introducing terms, such as "computer crime", "high-tech crime", "virtual crime", and "net crime", as many tried to determine whether cybercrime should constitute a new category of crime or the "old" categories should simply be adapted to the digital world [154]. In the precious chapter, both negative and positive consequences of the last idea have already been described, however, this debate remains relevant in the context of international criminal accountability, as the way cyber conduct is classified directly affects the legal framework applicable to it. If cyber operations are viewed merely as digital versions of existing offences, current legal categories may be sufficient in some cases.

At the same time, the unique features of cyber conduct may expose gaps in traditional legal concepts and challenge already established concepts of attribution, sovereignty, and legal responsibility. Not to mention that even orthography, spelling rules, may hint at the characteristics or meaning of the term. As some scholars suggest, the prefix "cyber" has already lost its earlier positive associations as it stopped being used to describe ordinary everyday activities, therefore the predominant spelling has changed from "cyber crime" to "cybercrime" as a single word because the term has become more closely associated with harmful or unlawful conduct in the digital sphere[155], and the daily vocabulary switched to the adjective "digital". Back in 2004, Wall described this complexity of definitions and terms with much simplicity "whatever its merits and demerits, the term 'cybercrime' has entered the public parlance and we are more or less stuck with it."[156]

However, based on these discussions, the theoretical and practical understanding of cybercrime remain remained open to interpretation. In 2013 the UK Home Office published a report formalizing and mainstreaming the distinction between cyber-

---

[153] Ibid. p. 118-143.
[154] Jonathan Lusthaus, "Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?," *Annual Review of Law and Social Science* 20 (2024), p.369. https://www.annualreviews.org/content/journals/10.1146/annurev-lawsocsci-041822-044042#right-ref-B83
[155] Kirsty Phillips, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken, "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies," *Forensic Sciences* 2, no. 2 (2022): 379.
[156]David Wall, "What are Cybercrimes?," *Criminal Justice Matters* 58, no. 1 (2004): 20.

dependent and cyber-enabled offences[157]. It became a baseline framework for categorizing cyber conduct and put the distinction proposed by the Explanatory Report to the Budapest Convention on Cybercrime into specific terms, they were later used for the OTP Policy on CEC. The cyber-dependent crimes are crimes that "can only be committed using a computer, computer networks or other form of information communications technology"[158]. Examples of include spreading viruses or other malware, hacking or DDoS attacks. In contrast, cyber-enabled crimes are traditional crimes that generally happen in the offline environment, but "can be increased in their scale or reach by use of computers, computer networks or other forms of ICT", such as data theft or electronic fraud[159].

This is also the term that was chosen by the OTP for the Policy on CEC. It was implemented with an almost identical meaning and purpose – "to refer to crimes within the jurisdiction of the Court – that is genocide, crimes against humanity, war crimes and aggression, as set out in article 5 of the Rome Statute, or offences against the administration of justice at the Court under article 70, when these crimes are committed or facilitated with the use of cyber means."[160]

A wide variety of terms that can be used to define cybercrime, while pushing the doctrinal development, has also contributed to a significant degree of conceptual fragmentation.[161] This can lead to challenges in achieving the level of clarity and consensus needed for the creation of a separate provision on cybercrime within the Rome Statute. Whether such provision is truly needed is a question that will be

---

[157] Jonathan Lusthaus, "Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?," *Annual Review of Law and Social Science* 20 (2024), p.369. Accessed April 11, 2026 https://www.annualreviews.org/content/journals/10.1146/annurev-lawsocsci-041822-044042#right-ref-B83

[158] McGuire, Mike, and Samantha Dowling. *Cyber Crime: A Review of the Evidence*. Home Office Research Report 75. Chapter 1: Cyber-Dependent Crimes. London: Home Office, October 2013. https://assets.publishing.service.gov.uk/media/5a7c83c1ed915d48c241043f/horr75-chap1.pdf

[159] McGuire, Mike, and Samantha Dowling. *Cyber Crime: A Review of the Evidence*. Home Office Research Report 75. Chapter 2: Cyber-Enabled Crimes — Fraud and Theft. London: Home Office, October 2013. https://assets.publishing.service.gov.uk/media/5a755a94e5274a59fa7177f7/horr75-chap2.pdf

[160] International Criminal Court, Office of the Prosecutor. "Questions and Answers: The ICC Office of the Prosecutor's Policy on Cyber-Enabled Crimes under the Rome Statute." 3 December 2025. https://www.icc-cpi.int/about/otp/questions-and-answers-the-icc-office-of-the-prosecutors-policy-on-cyber-enabled-crimes-under-the-rome-statute

[161] Kirsty Phillips, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken, "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies," *Forensic Sciences* 2, no. 2 (2022): 379. https://doi.org/10.3390/forensicsci2020028.

analyzed in the second part of this chapter, but more and more scholars continue to highlight the need for unified definitions[162], some even proposing the changes to how the well-established within the Rome Statute are defined, for example, aggression[163].

Another key limitation of contemporary ICL regarding cybercrimes is *mens rea*. Under Article 30 of the Rome Statute, liability depends on intent regarding conduct and knowledge of consequences and circumstances. This means that the perpetrator must act with awareness that harm will occur in the ordinary course of events.[164] This article refers to specific elements such as "intent" and "knowledge", leaving out traditional "recklessness", as the travaux préparatoires of the Rome Conference could not achieve a consensus on the definitions and appropriateness of the application in the Rome Statute[165]. The establishment of the "intent" and "knowledge" concepts together supports a popular view in contemporary international criminal law that, generally, a person is unable to perform an action that causes consequences unless they have knowledge of the circumstances in which that action was committed[166].

The idea of punishing those with a guilty mind is well grounded in the principles of justice and non-violation of human rights[167]. However, many scholars highlight that the traditional understanding of *mens rea* for cyber operations and automated weapon systems sets the bar too high[168]. Cyber operations, especially those that involve AI, often produce unpredictable and widespread effects, which undermine the requirement of knowledge. Cyberattacks can spread beyond intended targets or end in unintended ways, which makes it difficult to prove that the perpetrator had the necessary "virtual certainty" of outcomes. But the traditional understanding of *mens rea* might not only

---

[162] Xin Wang, "Global (Re-)Framing of Cybercrime: An Emerging Common Interest in Flux of Competing Normative Powers?," *Leiden Journal of International Law* 38, no. 2 (2025): 235. https://doi.org/10.1017/S0922156524000402.

[163] Jonathan A. Ophardt, "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield," *Duke Law & Technology Review* 9 (2010). https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1198&context=dltr

[164] *Rome Statute of the International Criminal Court*, adopted 17 July 1998, entered into force 1 July 2002, 2187 UNTS 90, art. 30. Accessed April 14, 2026. https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf

[165] Otto Triffterer and Kai Ambos, "The Rome Statute of the International Criminal Court: A Commentary," 3rd ed. (2016): 1122.

[166] Anna Rosalie Greipl, "Data-Driven Learning Systems and the Commission of International Crimes: Concerns for Criminal Responsibility?," *Journal of International Criminal Justice* 21, no. 5 (2023): 1097

[167] Thompson Chengeta, "Accountability Gap, Autonomous Weapon Systems and Modes of Responsibility in International Law" Harvard Law School, (2015): 18.

[168] Ibid, p. 19-20.

be inadequate, but also but also sets an unrealistically high threshold in the context of cyber operations. As a result, strict requirements of intent may fail to capture situations where actors knowingly take risks or deploy tools that can cause widespread harm, even if specific outcomes were not fully intended.

3.1.2. Limits in comparison to national legislation

The comparison of international criminal law to Ukrainian criminal law in terms of means rea also reveals some differences. Not only the forementioned recklessness, but also negligence, which, although present in the draft of the Statute[169], are not a part of the current Rome Statute's elements of *mens rea*. Under the Criminal Code of Ukraine, recklessness (самовпевненість) is understood as a form of negligence where a person foresees the possibility of harmful consequences but carelessly relies on their prevention[170]. In this case, the individual is aware of the risk, yet unjustifiably assumes that the negative outcome will not occur. Negligence (недбалість), in contrast, arises where a person does not foresee the possibility of harmful consequences, although they should have and could have foreseen them given the circumstances[171]. Here, liability is based not on actual awareness, but on a failure to exercise the required level of care.

The drafting history of the Rome Statute shows that although some proposals initially included these two concepts, there was no consensus among states, and these concepts were considered too uncertain and controversial for crimes of such gravity. This decision was, as scholars suggest, tied not only to the lack of consensus, but most likely to the jurisdiction of the ICC itself, that was set out in Article 5[172]. In this article the Rome Statute asserts that the "jurisdiction of the Court shall be limited to the most serious crimes of concern to the international community as a whole"[173], therefore making somewhat less clear concepts of recklessness and negligence not sufficient

[169] Roger S. Clark, "The Mental Element in International Criminal Law: The Rome Statute of the International Criminal Court and the Elements of Offences," *Criminal Law Forum* 12 (2001): 291-334.
[170] Criminal Code of Ukraine [Кримінальний кодекс України]. Law No. 2341-III. 5 April 2001. Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[171] Ibid.
[172] Roger S. Clark, "The Mental Element in International Criminal Law: The Rome Statute of the International Criminal Court and the Elements of Offences," *Criminal Law Forum* 12 (2001): 291-334.
[173] *Rome Statute of the International Criminal Court*, adopted 17 July 1998, entered into force 1 July 2002, 2187 UNTS 90, art. 30. Accessed April 14, 2026. https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf

enough to for the most serious crimes[174]. The exclusion of negligence can be also justified by its nature, as it involves a lower degree of culpability compared to intent or even recklessness, as the perpetrator does not actually anticipate the harmful outcome. In this sense, limiting liability to intent and knowledge can be seen as a way to ensure that only individuals with a high level of awareness and responsibility for their actions are held accountable under international criminal law.

The exclusion of the concept of recklessness still raises certain questions, as scholars continue to criticize such decision[175]. Even in traditional warfare, there are situations where actors proceed despite being aware of significant risks, without necessarily intending a specific harmful outcome. For instance, a commander orders an airstrike on a military target located in a densely populated urban area, aware that civilian casualties are likely, even though harming civilians is not the intended objective.

A similar pattern preserves in the context of cyber operations, as the deployment of malware or other intrusive tools may be directed at a particular target, however, the actor is aware that the effects could spread beyond the intended system. For example, cyberattacks may unintentionally affect interconnected networks, critical infrastructure, or third-party systems due to the interconnectness and interdependence of digital environments, which was described in Chapter 1. In such cases, although the actor may not intend the full scope of the harm, they may still proceed with the operation despite foreseeable risks. For example, when a cyber operation is deployed to disrupt a military communications system, knowing that the same network also supports a civilian hospital. This type of conduct could introduce conscious risk-taking rather than simple direct intent to the Rome Statute, but the ICC does not support the position that it is enough for the perpetrator to be aware of the risk that their conduct has[176], as of now.

---

[174] Roger S. Clark, "The Mental Element in International Criminal Law: The Rome Statute of the International Criminal Court and the Elements of Offences," *Criminal Law Forum* 12 (2001): 291-334.
[175] Johan Van der Vyver, "The International Criminal Court and the Concept of Mens Rea in International Criminal Law" *University of Miami International & Comparative Law Review*, Vol. 12, (2004): 57-94, 2004,
[176] Ibid, 57-94.

At the same time, adopting such an approach, similar to the character-based perspective on cyber attacks, could potentially open a "Pandora's box" by significantly complicating investigations and the process of proving individual responsibility. Expanding the scope of *mens rea* to include broader forms of risk awareness may create uncertainty and make it more difficult to establish clear standards of liability[177], so it may still be preferable to stick to the classical understanding of *mens rea* based on intent and knowledge. Nevertheless, it remains important to acknowledge that under this strict framework, certain actions that cause serious harm, comparable in their consequences to the most serious international crimes, may fall outside the scope of international criminal responsibility.

3.1.3 Limits within the group and leadership responsibility

One of the other limitations of ICL in the context of cyber warfare also lies in its difficulty in addressing forms of collective and distributed conduct that do not fit within traditional frameworks of international individual criminal responsibility. Cybersecurity studies suggest that most of the cybercrime groups do not have a specific leader, rather they have a couple of the most stable core members who have been committing cybercrimes together over an extended period of time, with occasional members joining for specific "missions"[178]. Therefore, cybercrime has always been increasingly group-based, transnational, and networked, rather than individual. For example, a single cyber operation may involve programmers who develop malicious code, operators who deploy it, state officials who authorize or tacitly support the activity, and third-party actors, sometimes loosely affiliated or even independent, who contribute to its execution. In addition, the increasing use of automated scripts and artificial intelligence further complicates the attribution of conduct, as certain actions may be executed without continuous human intervention or may evolve dynamically after deployment. This reflects a broader challenge already recognised in ICL, where crimes are often committed through collective structures involving multiple actors,

[177] Roger S. Clark, "The Mental Element in International Criminal Law: The Rome Statute of the International Criminal Court and the Elements of Offences," *Criminal Law Forum* 12 (2001): 291-334.
[178] Jason R. C. Nurse and Maria Bada, "The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations," in *The Oxford Handbook of Cyberpsychology* (Oxford University Press, 2019). https://doi.org/10.1093/oxfordhb/9780198812746.013.36.

making it difficult to clearly assign individual responsibility within a wider system of coordinated action.[179]

At the same time, ICL still insists on individual accountability, even in situations of what is often described as "system criminality," where crimes are carried out through organised or loosely coordinated groups[180]. This creates a tension between the collective nature of such crimes and the need to attribute responsibility to specific individuals, especially when actions are dispersed across networks rather than structured hierarchies[181]. More broadly, this also shows, a wrong for most cybercrime groups, underlying assumption of hierarchical organization that does not align well with the networked nature of cyber activities. At its core, ICL is built on the idea of individual culpability, meaning that liability must be personal, grounded in a sufficiently direct contribution to a crime, and accompanied by the required mental element[182]. However, cyber operations often have both the actus reus and the *mens rea* elements spread out across multiple actors, making it difficult to satisfy the requirement. For example, one actor may design malware without knowledge of its eventual use, another may deploy it without understanding its full consequences, while a third may benefit from or coordinate the broader operation without engaging in any technically executable act. Unlike traditional contexts, where assistance is more visible and close in time to the crime, in cyber operations contributions may be remote, indirect, or even repurposed across multiple incidents, raising questions about whether they meet the threshold of "substantial effect" typically required in criminal law.

3.1.4 Limits within the modes of liability

Moreover, doctrines like joint criminal enterprise rely not only on participation but also on a shared intent, or as the ICTY put it "existence of a common plan, design, or purpose"[183] which becomes difficult to establish in decentralized cyber

---

[179] Douglas Guilfoyle, "Responsibility for Collective Atrocities: Fair Labelling and Approaches to Commission in International Criminal Law," *Current Legal Problems* 64, no. 1 (2011): 255-286.
[180] Ibid, p. 256.
[181] Ibid, p. 257.
[182] Werle, Gerhard, and Florian Jeßberger. "Principles of International Criminal Law". 4th ed. Oxford: Oxford University Press, 2020. https://doi.org/10.1093/law/9780198826859.001.0001.
[183] *Prosecutor v. Duško Tadić*, Case No. IT-94-1-A, Judgment (ICTY Appeals Chamber, 15 July 1999), para. 227. https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf

environments. National criminal law, including Ukrainian, traditionally requires that co-perpetrators possess a degree of mutual awareness and coordination[184]. Yet in cyber contexts, actors may operate in parallel rather than in concert, contributing to a harmful outcome without any clear agreement or even knowledge of each other's existence. Similarly, command responsibility, as was developed in cases such as *Prosecutor v. Delalić et al*., depends on the notion of effective control, meaning that a superior has the material ability to prevent or punish the actions of subordinates[185]. In cyber operations, however, this control is often informal or spread between many members of the group. States may rely on loosely affiliated hacker groups or private actors[186], where influence exists but does not rise to the level of legal control required to trigger responsibility. This creates a gap where harmful conduct may take place within a broader sphere of influence, yet still falls outside the scope of existing criminal law doctrines, which require a clearer link between the individual and the prohibited act.

Also, in many cyber groups, actors are functionally interchangeable, meaning that the removal of one participant does not prevent the operation. This shows a practical shift from individual causation to what might be described as system-based causation, or system criminality, where the outcome depends on the continued functioning of the network rather than on any single actor[187]. As a result, it becomes difficult to identify an indispensable or also called essential contribution, which is often required, as was highlighted in the ICC's practice, specifically in the case *Prosecutor v. Thomas Lubanga Dyilo*, such as co-perpetration based on control over the crime[188].

In addition to these doctrinal challenges, there remain numerous procedural issues that further limit the application of international criminal law in the cyber

---

[184] Criminal Code of Ukraine [Кримінальний кодекс України]. Law No. 2341-III. 5 April 2001. Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[185] *Prosecutor v. Zejnil Delalić, Zdravko Mucić, Hazim Delić and Esad Landžo* (*Čelebići*), Case No. IT-96-21-T, Trial Chamber Judgment (ICTY, 16 November 1998), para. 348-377. https://www.icty.org/x/cases/mucic/tjug/en/

[186] Jason R. C. Nurse and Maria Bada, "The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations," in *The Oxford Handbook of Cyberpsychology* (Oxford University Press, 2019). Accessed April 20, 2026. https://doi.org/10.1093/oxfordhb/9780198812746.013.36.

[187] Douglas Guilfoyle, "Responsibility for Collective Atrocities: Fair Labelling and Approaches to Commission in International Criminal Law," *Current Legal Problems* 64, no. 1 (2011): 255-286.

[188] *Prosecutor v. Thomas Lubanga Dyilo*, Case No. ICC-01/04-01/06, Trial Chamber I, Judgment pursuant to Article 74 of the Statute (ICC, 14 March 2012), para.922., https://www.worldcourts.com/icc/eng/decisions/2012.03.14_Prosecutor_v_Lubanga1.pdf

context, many of which originate from the unique characteristics of cyberspace itself, such as anonymity, jurisdictional fragmentation, and evidentiary complexity. However, the most central limitations lie in the divergence of definitions, the difficulty of establishing *mens rea*, and the problem of collective and distributed responsibility. These issues are not isolated, but rather closely connected to broader challenges already present in the prosecution of other international crimes, where similar tensions between individual liability and collective harm continue to shape the development of the law.

3.2 Reinterpreting the Rome Statute in the context of cyber operations and the new OTP framework

The ICC Rome Statute was designed as a carefully negotiated and relatively closed legal framework, built to address the most serious crimes that concern the international community. However, the Statute's structure and contents reflect a compromise between legal precision and political feasibility, prioritizing stability, legitimacy, and state consent over rapid adaptability[189]. While this design has contributed to the durability and legitimacy of ICL, it also gives rise to noticeable tension when the framework is applied to continuedly evolving areas and newly emerging forms of conduct in modern society. The problem is not simply that new types of harmful behavior and means to perpetrate it continue to develop, but rather that the underlying institutional logic of the Rome Statute is not designed for quick adaptation. Instead, it operates through a system that is inherently cautious and slow-moving, which makes it difficult to respond effectively to technological developments, such as cyber operations, that evolve at a much faster pace[190]. This characteristics of the Statute is not unique to the cybercrime: ecocide is one of the other crimes that has already been criminalized in many countries within their national criminal law but not

[189] Otto Triffterer and Kai Ambos, eds., "The Rome Statute of the International Criminal Court: A Commentary", 3rd ed. (2016): 1122.
[190] William A. Schabas, "The International Criminal Court: A Commentary on the Rome Statute", *2nd ed*. (Oxford University Press, 2016). https://academic.oup.com/oxford-law-pro/book/57464

yet within the Rome Statute, even though there has already been a formal proposal to add it to the Statute [191].

In late 2025, the OTP released the Policy on Cyber-enabled Crimes.[192] It has given the OTP a comprehensive strategy for addressing crimes committed through cyber means. To understand this important practical step, it is crucial to analyze which approaches scholars proposed for interpreting the Rome Statute in connection to cybercrimes. Most of these proposals were not aimed at importing ordinary domestic understandings and criminal norms of "cybercrime" into the Rome Statute. Rather, scholars proposed to explore whether the conduct committed through cyber means could already fall within genocide, crimes against humanity, war crimes, or aggression, and if not, whether the Statute should be amended to address the gap more directly[193]. The pre-policy period can be best understood as a debate between interpretation and reform: one camp argued that the existing Statute was technologically neutral enough to encompass at least the gravest cyber conduct, while the other argued that the digital age exposed structural omissions that should be corrected or amended fully.

3.2.1 Pre-policy approaches to cybercrimes

The dominant proposal before the policy was interpretive rather than legislative, meaning that its core idea encompassed the interpretation of the existing norms to fit the new domain. Many scholars believe that there is no need to create a standalone Rome Statute crime of "cybercrime". Instead, cyber operations should be assessed under the existing crimes frameworks if their effects, context, and gravity satisfy the established legal elements[194]. As it often happens, there was no clear consensus on what effects and gravity the cyber operation should have in order to be assessed under one of the Rome Statute articles, but there was an agreement on what It should not. As Hathaway reflects: "Suffice it to say that there are, as of this writing, significant differences among experts on the matter. There is agreement, however, that cyber

[191] Ritwik Sharma, "Ecocide as the Fifth International Crime: Is the Rome Statute Compatible with Ecocide?," *Völkerrechtsblog*, 16 January 2025. https://voelkerrechtsblog.org/ecocide-as-the-fifth-international-crime/
[192] "ICC OTP Issues First Policy on Cyber-Enabled Crimes," *International Law in Brief*, American Society of International Law, 13 January 2026. https://asil.org/ilib/icc-otp-issues-first-policy-cyber-enabled-crimes/
[193] "Cyberwarfare Issue: When Might Cyber Operations Constitute Crimes Under the Rome Statute?," *ICC Forum*, UCLA School of Law Promise Institute, March–July 2022. https://iccforum.com/cyberwar
[194] Ibid.

operations with mere economic effects would not be sufficient to constitute a crime of aggression."[195] Roscini argued that within this interpretative approach, there is "no need to amend" Article 8 in order to prosecute cyber war crimes, because the real difficulties lie in attribution and evidence rather than in the definition of war crimes itself.[196] Building on this, it can be argued that much of the perceived "gap" in the Rome Statute is not normative, but more operational: the law may already be capable of covering certain forms of cyber conduct, yet its effective application is constrained by the unique characteristics of cyberspace that the Rome Statute was not designed for.

This position of interpretation of the current Statute was strongly reflected in the 2021 Council of Advisers' Report on the application of the Rome Statute to cyberwarfare. The report examined aggression, war crimes, crimes against humanity, and genocide, and concluded that cyber operations could in principle satisfy the relevant elements of those crimes[197]. The Report did not argue for an immediate amendment of the Statute, not because it is a long and complicated process, but the existing legal framework is, at least formally, technologically neutral. In other words, the Rome Statute does not require that harm be inflicted through kinetic means, what matters is whether the conduct, regardless of the method used, fulfills the material and contextual elements of the crime. For example, within Article 8bis on crime of aggression, the Council of Advisers highlighted that the list given in the article is not exhaustive and even if it was, it can be interpreted in a way to apply to cyber operations, making an already existing article of the Rome Statute applied to the specific conduct irrespective of whether the act was kinetic or non-kinetic[198].

In relation to war crimes, the Report suggested that cyber operations may qualify as "attacks" if they result in consequences comparable to traditional military operations[199]. The key point here is not the physical form of the act, but its effects: if a

---

[195] Ibid.
[196] Ibid.
[197] Permanent Mission of Liechtenstein to the United Nations, *The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare* (Global Institute for the Prevention of Aggression, August 2021). https://crimeofaggression.info/wp-content/uploads/GIPA_The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf
[198] Ibid, p. 26.
[199] Ibid, p. 27.

cyber operation leads to death, injury, or the destruction of objects protected under international humanitarian law, then it may fall within Article 8bis of the Rome Statute[200]. At the same time, the Report acknowledged existing doctrinal tensions, particularly around whether purely non-physical harm can meet the threshold of an "attack" under IHL. The report also highlighted that many issues regarding cyber operation damage, for example damage to critical infrastructure, are still unsettled because of those tensions and the risk of diluting the use of force threshold[201]. These mixed conclusions reflect academic uncertainty that existed in pre-policy debates. While the Statute may be interpreted flexibly, the underlying legal concepts were developed in a pre-digital context. Therefore, the proposed cyber-focused interpretation of the Statute might go beyond what was originally put into the meaning of the articles.

With respect to crimes against humanity, the Report adopted a similarly inclusive approach. It emphasized that cyber operations could form part of a "widespread or systematic attack directed against any civilian population" under Article 7, especially where they are used as tools to facilitate persecution, repression, or other inhumane acts[202]. For example, large-scale cyber surveillance, coordinated disinformation campaigns, or the targeting of specific groups through digital means could, depending on the circumstances, contribute to crimes against humanity. The Report moved beyond the idea of cyber operations as isolated technical acts and instead situated them within broader patterns of conduct[203]. This is important because crimes against humanity are defined not only by the act itself, but by the context in which it occurs. Cyber operations, when integrated into state policy or organized campaigns, as other academic works also highlight, may and could satisfy the contextual elements even if the individual acts appear less severe when viewed in isolation[204].

[200] Ibid, p. 9.
[201] Ibid, p. 15.
[202] Ibid, p. 67.
[203] Ibid, p. 4-88.
[204] Luís Matos, "Cyberattacks as Crimes Against Humanity and International Responsibility of States" (2021): 3-34.

And in relation to genocide, the Report was more cautious but did not exclude the possibility entirely[205]. It recognized that cyber operations could, in theory, contribute to genocidal acts, particularly where they are used to facilitate or amplify conduct such as incitement or the deliberate infliction of conditions of life calculated to bring about the destruction of a group[206]. However, the threshold for genocide remained exceptionally high, especially due to the requirement of specific intent (dolus specialis).

However, the analysis of the proposals withing the forementioned Report reveals additional limits of this approach. The ability to interpret the existing norm and applying them to cyber conduct depends heavily on how expansively the core elements, such as "attack," "use of force," or "widespread or systematic conduct", are interpreted in a non-kinetic context. This creates a degree of interpretative strain, especially where harm is indirect, delayed, or primarily affects infrastructure rather than individuals in an immediate physical sense. Moreover, while the Council proposed Article 8bis to be interpreted and read flexibly[207] and scholars reassuring that a cyber operation can constitute a manifest violation of the UN Charter[208], the threshold requirement of a manifest violation of the UN Charter remains a significant constraint within this approach, especially in cases where cyber operations produce disruption without clear physical destruction, like the pre- and post-2022 cyber operations against both critical Ukrainian infrastructure and civilian telecommunications and governmental institutions. This illustrates the broader point that the reliance on interpretation alone, while attractive from the perspective of legal stability and efficiency of the resources, may not fully resolve the problem arising between the structure of the existing ICL frameworks and the realities of cyber operations.

---

[205] Permanent Mission of Liechtenstein to the United Nations, *The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare*. Global Institute for the Prevention of Aggression, August 2021. https://crimeofaggression.info/wp-content/uploads/GIPA_The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf

[206] Ibid, p. 71-88.

[207] Ibid, p. 4-22.

[208] Marco Roscini,"Cyber Operations Can Constitute Was Crimes Under the ICC Jusrisdiction Without Need to Amend the Rome Statute" *ICC Forum*, UCLA School of Law Promise Institute, March–July 2022. https://iccforum.com/cyberwar

The legislative proposals of the pre-policy period were more limited, yet there were distinct ideas shared among different scholars that proposed changes to the Rome Statute rather than trying to fit crimes from a new domain with the existing norms that were not created for them in the first place. The scarcity of such approach can be explained by the complexity of the amendment process, as many scholars note, the amendment procedure requires broad state consent and reflects delicate compromises between states, which makes any expansion, especially into technologically complex and politically manipulated areas like cyber domain, both time-consuming and uncertain.

One of the reforming proposals is centered on amending the existing crimes rather than creating a fully new and autonomous "cybercrime" category. Scheffer stresses that the current definition of aggression is outdated and incomplete, because it is based on the 1974 UN General Assembly definition and therefore reflects a purely kinetic, state-centric understanding of force[209]. The scholar calls the absence of cyber operations a "glaring omission" that ignores modern realities of warfare and creates a legal environment in which the ICC may be unable to investigate or prosecute acts of aggression carried out through cyber means alone[210]. His suggestion of amendment lies in inclusion of cyber operations, such as disabling infrastructure, shutting down power grids, denial-of-service attacks etc., into the definition of the crime of aggression[211]. This requires minimal changes to the article 8bis, but at the same time allows to address the "elephant in the room"[212].

His suggested changes go as follows:

> Article 8bis (1): For the purpose of this Statute, "crime of aggression" means the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political, or military, ***or cyber action*** of a State ***or non-State entity***, of an act of aggression which, by its

[209] David Scheffer, "The Missing Pieces in Article 8 *bis* (Aggression) of the Rome Statute," *Harvard International Law Journal* 58, Online Journal (2017): 84.
[210] Ibid, p. 84.
[211] Ibid, p. 83-85.
[212] Ibid, p. 85.

character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations.

Article 8bis (2):

(h) The use of cyber measures for an offensive purpose that significantly disrupts or degrades governmental, military, commercial, cultural, or media entities or other societal activities in another State[213].

At the same time, other scholars approached legislative reform even more cautiously, emphasizing that any amendment must preserve the coherence and legitimacy of the existing system[214]. For example, Miller examined the implications of the Kampala amendments and argued that while cyberattacks could, in principle, fall within the existing definition of aggression, there is the lack of explicit reference to cyber conduct leaves significant interpretive uncertainty.[215] Rather than proposing a fully new offence, her analysis highlights the possibility of textual clarification through interpretive guidance or narrowly framed amendments that would signal or imply the inclusion of cyber operations but without fundamentally restructuring the provision or expanding its body[216]. Such cautious approach can be seen as a parallel to the earlier mentioned Report on the application of the Rome Statute to cyberwarfare. The scholar highlights the lack of explicit textual reference to cyber operations as a source of ambiguity within Article 8*bis* [217], the Council of Advisers similarly identifies unresolved questions surrounding key concepts such as "use of force" and "attack."[218] Both approaches reflect an underlying concern that some amendments, especially if they are broad or fundamentally changing, could disrupt the carefully negotiated balance of the Rome Statute. That is the reason for suggesting a gradual clarification,

---

[213] David Scheffer,"Amending the Rome Statute to Cover Cyberwarfare as Aggression" *ICC Forum*, UCLA School of Law Promise Institute, March–July 2022.. https://iccforum.com/cyberwar

[214] Kevin L. Miller, "The Kampala Compromise and Cyberattacks: Can There Be an International Crime of Cyber-Aggression?," *Southern California Interdisciplinary Law Journal* 23 (2014): 217-260.

[215] Ibid, p.232-234.

[216] Ibid, 217-260.

[217] Ibid, p. 220-234.

[218]Permanent Mission of Liechtenstein to the United Nations, *The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare* (Global Institute for the Prevention of Aggression, August 2021). https://crimeofaggression.info/wp-content/uploads/GIPA_The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf

whether through jurisprudence, policy, or limited textual adjustment, since it offers a more cautious, but still clear path for integrating cyber operations into the existing legal framework.

Overall, the pre-policy period was marked by a clear tension between interpretive flexibility and cautious legislative innovation, with most scholars recognizing that cyber operations expose structural gaps in the Rome Statute but disagreeing on how far reform should go. While some proposed targeted amendments or even new offence categories, these ideas remained fragmented and largely theoretical, constrained by concerns over legality, coherence, and the political difficulty of amending the Statute. Against this background of conceptual uncertainty and limited consensus, the emergence of the OTP Policy on Cyber-Enabled Crimes represents a shift from academic debate to institutional clarification of how existing law should operate in the digital context.

3.2.2 OTP Policy's approaches to cybercrimes

The Policy does not introduce new crimes or amend the Statute. Instead, it consolidates and proposes ways to apply the interpretive approach that has become more popular among the academic community. In doing so, the Policy confirms that cyber-enabled conduct can fall within the Court's jurisdiction where it satisfies the elements of genocide, crimes against humanity, war crimes, or aggression.

The Policy adopts a technology-neutral approach, reaffirming that the Rome Statute is not limited to kinetic or physically destructive conduct[219]. In this respect, the Policy aligns closely with earlier interpretive positions advanced in academic literature and the 2021 Council of Advisers' Report, but goes further by embedding these ideas into a structured strategy for prosecution. The Policy recognizes that cyber technologies may be used both as tools and as enabling environments, broadening the analytical lens through which criminal conduct is assessed[220]. But a key conceptual contribution of the Policy lies in its distinction between "cyber-dependent" and "cyber-

[219] Harriet Moynihan, "Securing Justice for Cyber-Enabled International Crimes," *Just Security*, 3 February 2026. https://www.justsecurity.org/129752/justice-cyber-international-crimes/
[220] Ibid.

enabled" crimes, as this destinction and the OTP's definition of the terms will most likely become custom within the international criminal law after some time. Cyber-dependent crimes are those that can only be committed through digital systems, such as hacking or the deployment of malware[221]. Cyber-enabled crimes, by contrast, are traditional offences, for example, attacks against civilians, that are facilitated or amplified through cyber means[222]. The OTP Policy focuses primarily on the second category[223], reflecting the jurisdictional limits of the ICC. This distinction is important because it allows the Prosecutor to engage with cyber conduct without transforming the Court into a general institution for international cybercrime, like cyber fraud, hacking or identity theft[224]. Instead, the focus stays on core international crimes, with cyber technology seen simply as a way those crimes are carried out.

In relation to war crimes, the Policy clarifies that cyber operations may qualify as "attacks" where they result in consequences comparable to kinetic military action[225]. This includes not only physical destruction or injury, but also functional impairment of objects, particularly where such impairment affects critical civilian infrastructure. For example, a cyber operation that disables a hospital's systems, disrupts electricity supply, or interferes with water distribution may be assessed as an attack under international humanitarian law if it produces sufficiently severe effects. The Policy therefore moves beyond a strictly physical understanding of harm and embraces a more functional and effects-based interpretation, while still emphasizing that not all cyber disruptions will meet the threshold required for war crimes[226].

---

[221] McGuire, Mike, and Samantha Dowling. *Cyber Crime: A Review of the Evidence*. Home Office Research Report 75. Chapter 1: Cyber-Dependent Crimes. London: Home Office, October 2013. https://assets.publishing.service.gov.uk/media/5a7c83c1ed915d48c241043f/horr75-chap1.pdf

[222] McGuire, Mike, and Samantha Dowling. *Cyber Crime: A Review of the Evidence*. Home Office Research Report 75. Chapter 2: Cyber-Enabled Crimes — Fraud and Theft. London: Home Office, October 2013. https://assets.publishing.service.gov.uk/media/5a755a94e5274a59fa7177f7/horr75-chap2.pdf

[223] ICC Office of the Prosecutor, *Policy on Cyber-Enabled Crimes under the Rome Statute* (ICC, December 2025). https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf

[224] DiploFoundation. "International Criminal Court (ICC) Issues Policy on Cyber-Enabled Crimes." *Digital Watch Observatory*. 13 December 2025. Accessed April 21, 2026 https://dig.watch/updates/international-criminal-court-icc-issues-policy-on-cyber-enabled-crimes

[225] ICC Office of the Prosecutor, *Policy on Cyber-Enabled Crimes under the Rome Statute* (ICC, December 2025), para. 80. https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf

[226] Ibid, para. 80-96.

The Policy also provides important clarification in relation to crimes against humanity, particularly the contextual requirement of a widespread or systematic attack directed "against any civilian population."[227] It recognizes that cyber-enabled conduct, such as mass surveillance, coordinated disinformation campaigns, or digital persecution, can form part of such an attack when carried out pursuant to a state or organizational policy. This reflects a broader shift in understanding the nature of "attack" in international criminal law, as cyber means may not only directly constitute criminal acts, but also facilitate and amplify traditional crimes, including through coordinated campaigns that operate across digital environments and physical realities simultaneously[228]. In doing so, the Policy acknowledges that individual cyber acts, which may appear minor in isolation, can collectively contribute to large-scale violations when embedded within a broader campaign[229].

While the Policy appropriately aligns with existing jurisprudence, it arguably adopts an overly restrictive view by treating cyber conduct primarily as supportive rather than constitutive of the "attack."[230] This risks overlooking situations in which coordinated cyber operations themselves form the core of a widespread or systematic attack against a civilian population. Therefore, there is a need for an approach that would recognize that large-scale cyber campaigns, such as sustained infrastructure disruption or coordinated information control, can independently meet the contextual threshold, particularly when their effects extend across both digital and physical domains[231].

With respect to genocide, the Policy adopts a more cautious tone, consistent with existing jurisprudence. It acknowledges that cyber-enabled conduct may play a role in genocidal processes, particularly in relation to incitement or the creation of conditions

---

[227] Ibid, para. 66.
[228] Marko Milanovic, "ICC Office of the Prosecutor Releases Draft Policy on Cyber-Enabled Crimes," *EJIL: Talk!*, 4 April 2025. https://www.ejiltalk.org/icc-office-of-the-prosecutor-releases-draft-policy-on-cyber-enabled-crimes/
[229] ICC Office of the Prosecutor, *Policy on Cyber-Enabled Crimes under the Rome Statute* (ICC, December 2025), para. 62-78. https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf
[230] Joanna Kulesza, "ICC Cyber-Enabled Crimes and DNS Abuse: Accountability Questions for Infrastructure Operators," *CircleID*, 18 December 2025. https://circleid.com/posts/icc-cyber-enabled-crimes-and-dns-abuse-accountability-questions-for-infrastructure-operators
[231] NATO Cooperative Cyber Defence Centre of Excellence. "Scenario 34: Crimes against Humanity." *International Cyber Law: Interactive Toolkit*. https://cyberlaw.ccdcoe.org/wiki/Scenario_34:_Crimes_against_humanity

of life calculated to bring about the destruction of a group[232]. At the same time, the Policy highlights that the specific intent requirement remains a high threshold, and that the use of cyber means does not alter this fundamental element[233]. As a result, while cyber technologies may facilitate genocidal acts, they are unlikely to constitute genocide independently unless accompanied by clear evidence of intent to destroy a protected group. It is hard to disagree with the OTP on the digital genocide, as the Policy states that "the Office considers it unlikely that a real-world scenario of genocide would be committed solely or primarily by cyber means"[234], especially considering the definition and the threshold of this crime. But the Policy is correct in acknowledging that it can play a role in genocidal processes as there are contemporary examples. Since the full-scale invasion, Russia has systematically tried not only to disrupt Ukrainian infrastructure through cyber operations, but also to reshape and erase Ukrainian identity in the information space. This includes cyberattacks targeting state databases [235] and media systems [236], as well as coordinated campaigns aimed at removing, altering, or replacing digital and physical records of Ukrainian cultural and historical presence[237].

The Policy's treatment of the crime of aggression is more restrained in comparison to the previously described crimes, reflecting the ongoing doctrinal uncertainty in this area. It acknowledges that cyber operations may, in principle, amount to acts of aggression if they meet the threshold of a "use of force" under international law [238]. However, it also recognizes that the current definition of

---

[232] Ibid.
[233] Ibid.
[234] ICC Office of the Prosecutor, *Policy on Cyber-Enabled Crimes under the Rome Statute* (ICC, December 2025), para. 57. https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf
[235] Yuliia Dysa, "Ukraine Says Russian Cyberattack Hits State Registries but No Data Lost," *Reuters*, 20 December 2024. https://www.reuters.com/technology/cybersecurity/ukraine-says-russian-cyberattack-hits-state-registries-no-data-lost-2024-12-20/
[236] Institute of Mass Information, "Russia's Crimes against the Media: At Least 100 Cyber Attacks on the Media and Journalists in the 3 Years since the Start of the Invasion," *IMI*, 21 February 2025. Accessed April 21, 2026. https://imi.org.ua/en/news/russia-s-crimes-against-the-media-at-least-100-cyber-attacks-on-the-media-and-journalists-in-the-3-i66765
[237] "Géopolitychna sytuatsiia zminylas': Yak Rosiia povnistyu zaboroniaie ukrainsku movu v shkolakh okupovanykh rehioniv" ["The Geopolitical Situation Has Changed: How Russia Is Completely Banning the Ukrainian Language in Schools in Occupied Regions"]. BBC News Ukraina, 26 June 2025. https://www.bbc.com/ukrainian/articles/cev0en0wnlpo.
[238]ICC Office of the Prosecutor, *Policy on Cyber-Enabled Crimes under the Rome Statute* (ICC, December 2025), para. 97-102. https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf

aggression in Article 8 bis does not explicitly address cyber conduct, and therefore requires careful interpretation. The Policy does not attempt to resolve these uncertainties definitively, but instead signals that the OTP will assess cyber operations in light of their scale, effects, and context, taking into account relevant developments in international law[239].

3.2.3 OTP Policy's approach to evidence and attribution within cybercrimes

Beyond doctrinal clarification, the Policy also highlights practical prosecutorial dimensions, especially the role of digital evidence and the procedural difficulties of investigating cyber-enabled crimes. In particular, the Policy makes clear that cyber conduct is relevant not only to how Rome Statute crimes are committed, but also to how evidence is generated, collected, and assessed, including situations involving digital interference with witnesses, evidence, or judicial proceedings[240]. This is especially important because digital evidence differs from more traditional forms of proof. It is often dispersed across servers, platforms, and service providers located in multiple jurisdictions; it may be volatile, easily altered, encrypted, or deleted; and it frequently requires specialized technical analysis before it can be translated into legally usable evidence. Scholars point out that the prosecution of cyber-enabled international crimes requires the ability to gather, preserve, authenticate, and analyse electronic material, as well as adequate training for investigators, prosecutors, and judges in digital forensics, attribution, encryption, blockchain tracing, and deepfake detection[241].

Closely connected to evidentiary difficulty is the problem of attribution. Factual attribution in cyberspace is exceptionally difficult because sophisticated actors route operations through compromised systems in multiple jurisdictions, use encryption, deploy false-flag techniques, and increasingly rely on AI-driven tools that may partially obscure the human chain of control[242]. As a result, the practical challenge is not simply

---

[239] Ibid, para. 97-102.

[240] Civil Society Alliances for Digital Empowerment, "International Criminal Court Issues Policy Clarifying Treatment of Cyber-Enabled Crimes under the Rome Statute," *CADE Project*, 10 December 2025. https://cadeproject.org/updates/international-criminal-court-issues-policy-clarifying-treatment-of-cyber-enabled-crimes-under-the-rome-statute/

[241] Wilmshurst, Elizabeth, Harriet Moynihan, and Tsvetelina van Benthem. "Securing Justice for Cyber-Enabled International Crimes: Legal Foundations and Practical Routes to Prosecution." *Chatham House*, (2026): p. 53-55.

[242] Devanshi Mehta, "Cyber-Enabled International Crimes and the Fragmentation of Jurisdictional Frameworks: Examining the ICC's 2025 Policy in the Context of Cross-Border Digital Warfare," *Record of Law*, 31 March 2026.

proving that harm occurred, but proving who is criminally responsible for that harm, under what mode of participation, and on the basis of what admissible evidence[243]. This is why the Policy must be read not only as a doctrinal document, but also as an acknowledgment of the severe operational barriers that cyber cases pose. Therefore, the Policy situates itself within a broader accountability framework by emphasizing cooperation beyond the Court itself. Experts also argue that successful prosecution of cyber-enabled international crimes requires cooperation between the ICC, states, cybercrime and war crimes units, private service providers, cybersecurity firms, and international organizations[244]. They specifically point to the need for cross-border evidence-sharing mechanisms, stronger domestic legal frameworks, reinforced cyber expertise across prosecution teams, and structured cooperation with private entities and expert networks[245]. This means that effective prosecution cannot depend on the ICC alone. Instead, it requires multi-level institutional coordination, because the relevant evidence, expertise, and investigative powers are distributed across a fragmented transnational landscape. In that sense, the Policy implicitly recognizes that accountability for cyber-enabled crimes is not only a matter of legal interpretation, but of building an operational system capable of turning technical traces into prosecutable cases[246].

The pre-policy period revealed a clear structural tension: while the Rome Statute was formally capable of addressing cyber-enabled conduct through interpretation, in practice the absence of guidance created uncertainty, fragmentation, and limited prosecutorial engagement with such acts. The adoption of the OTP Policy marked a shift from theoretical applicability to operational clarification, affirming that cyber means can constitute, facilitate, and evidence core international crimes without expanding the Court's jurisdiction. At the same time, the Policy implicitly

---

https://recordoflaw.in/cyber-enabled-international-crimes-and-the-fragmentation-of-jurisdictional-frameworks-examining-the-iccs-2025-policy-in-the-context-of-cross-border-digital-warfare/

[243] Ibid.

[244] Wilmshurst, Elizabeth, Harriet Moynihan, and Tsvetelina van Benthem. *"*Securing Justice for Cyber-Enabled International Crimes: Legal Foundations and Practical Routes to Prosecution*." Chatham House*, (2026): 46-49.

[245] Ibid, p. 61.

[246] ICC Office of the Prosecutor, *Policy on Cyber-Enabled Crimes under the Rome Statute* (ICC, December 2025). https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf

acknowledges that doctrinal recognition alone does not resolve the practical barriers to accountability, particularly in cases involving complex, large-scale cyber operations against critical infrastructure[247]. Therefore, the focus must move beyond interpretation toward the development of complementary mechanisms capable of addressing attribution, evidence, and enforcement challenges to find practical ways for establishing accountability for cyber attacks, including those that target critical infrastructure.

3.3 Application of the OTP framework to cyber operations against Ukrainian infrastructure

The practical relevance of the OTP Policy becomes particularly visible when applied to cyber operations targeting critical infrastructure in Ukraine. Since 2015, and especially following the full-scale invasion in 2022, Ukraine has been one of the most documented examples of large-scale coordinated state cyber activity directed against essential civilian systems, including electricity grids, telecommunications networks, governmental databases, and financial infrastructure. These operations provide a context in which the Policy's interpretive principles can be tested. In the Ukrainian context, cyber attacks on infrastructure are rarely isolated incidents, because they form part of a broader military and strategic campaign combining kinetic strikes and information warfare. This is precisely the type of environment in which the OTP Policy's emphasis on contextual and cumulative assessment becomes central. For example, repeated cyber intrusions into Ukraine's energy infrastructure, such as the 2015 and 2016 power grid attacks and subsequent operations using malware, demonstrate how cyber tools can produce real-world disruption to civilian life[248]. While not all such incidents would automatically meet the threshold of war crimes, the

[247] Ibid, para. 134.
[248] Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case* (E-ISAC/SANS, 18 March 2016). https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

Policy allows for their qualification as “attacks” where the functional consequences are sufficiently severe[249].

When applying the Policy, the key question is not whether physical destruction occurred, but whether the cyber operation resulted in consequences comparable to kinetic action. In Ukraine, disruptions to electricity supply during winter periods, particularly when coordinated with missile strikes, can directly affect hospitals, heating systems, water supply, and other essential services[250]. Under the OTP’s functional approach, such operations could fall within the notion of attacks against civilian objects, especially where the effects are foreseeable and disproportionately impact the civilian population . Moreover, the Ukrainian case illustrates how cyber operations targeting infrastructure may contribute to broader patterns of conduct relevant for crimes against humanity. The systematic nature of attacks on energy, communication, and administrative systems points toward a strategy aimed at destabilizing civilian life and undermining basic conditions of existence. In this respect, the Policy’s recognition that cyber-enabled acts can form part of a “widespread or systematic attack” becomes directly applicable, since repeated disruptions to infrastructure, when viewed cumulatively, may contribute to the intentional infliction of conditions of life that severely affect civilian populations, particularly in combination with other forms of violence[251].

At the same time, the Ukrainian case highlights the evidentiary potential and challenges of cyber operations, yet attribution remains perhaps the most difficult issue in applying the Policy. Many of the cyber operations conducted by anonymous groups targeting Ukrainian infrastructure have been linked to state-sponsored or affiliated groups[252], but establishing individual criminal responsibility within the framework of

---

[249] ICC Office of the Prosecutor, *Policy on Cyber-Enabled Crimes under the Rome Statute* (ICC, December 2025). https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf

[250] Oleksii Artemchuk, "Number of Cyberattacks on Ukraine Increased by 70% in Past Year," *Ukrainska Pravda*, 9 January 2025. Accessed April 21, 2026. https://www.pravda.com.ua/eng/news/2025/01/09/7492671/

[251] ICC Office of the Prosecutor, *Policy on Cyber-Enabled Crimes under the Rome Statute* (ICC, December 2025). https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf

[252] Anna Paskevych, [Анна Паскевич]. “U SBU rozkryly, khto stoit za kiberatakoyu na derzhreestry Ukrainy y chy mih statysia vytik danykh” [The SBU Revealed Who Is Behind the Cyberattack on Ukraine’s State Registries and Whether a Data Leak Could Have Occurred]. Obozrevatel, 20 December 2024. https://news.obozrevatel.com/ukr/society/u-sbu-rozkrili-hto-stoit-za-kiberatakoyu-na-derzhreestri-ukraini-j-chi-mig-statisya-vitik-danih.htm.

international criminal law requires a higher evidentiary threshold. The distributed nature of cyber operations, which often involves multiple actors, jurisdictions, and layers of obfuscation, complicates the identification of specific perpetrators and their modes of liability[253]. Nevertheless, the Policy's reliance on existing doctrines of participation, such as ordering, facilitating, or aiding and abetting, provides a legal pathway for addressing these complexities, even if practical implementation remains challenging.

Finally, the Ukrainian case shows the broader significance of the OTP Policy as a framework for future accountability. While no cases have yet been brought before the ICC specifically focused on cyber-enabled crimes, the situation in Ukraine provides a real-world testing ground for how such cases might be brought to the ICC. The International Criminal Court has issued arrest warrants in relation to attacks on energy infrastructure, marking one of the first instances where large-scale electric infrastructure disruption has been addressed within the Court's framework[254]. While the publicly available information does not explicitly focus on cyber aspects, it is reasonable to suggest that such operations, given their complexity and the known patterns of coordinated attacks on Ukrainian infrastructure, may have involved cyber components alongside kinetic means. This might also indicate that the distinction between cyber and traditional methods may become less significant in practice, as both can form part of a broader course of conduct. As a result, the Ukrainian example may serve as an early casestudy of how cyber-enabled elements could be integrated into existing legal frameworks, even if they are not explicitly identified as such in current proceedings.

[253] ICC Office of the Prosecutor, *Policy on Cyber-Enabled Crimes under the Rome Statute* (ICC, December 2025). https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf

[254] International Criminal Court, "Situation in Ukraine: ICC Judges Issue Arrest Warrants against Sergei Kuzhugetovich Shoigu and Valery Vasilyevich Gerasimov," 5 September 2024. Accessed April 21, 2026 https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-sergei-kuzhugetovich-shoigu-and

3.4 Emerging models of responsibility for cyber crimes

While the OTP Policy on Cyber-Enabled Crimes provides an important interpretive foundation for applying the Rome Statute to cyber operations, it does not in itself resolve the deeper structural challenges of accountability, because these attacks are characterized by distributed actors, proxy involvement, evidentiary complexity, and cross-border execution, which create a gap between legal qualification and practical enforcement. Despite the applicability of international criminal law, there remains a significant risk of impunity due to practical and institutional barriers to prosecution[255]. As a result, scholars and policymakers increasingly recognize that the ICC framework, even when supported by the OTP Policy, must be complemented by alternative or additional accountability mechanisms[256]. These include international tribunals, attribution bodies, strengthened domestic prosecutions, and hybrid institutional arrangements. Each of these options responds to specific weaknesses in the current system, particularly in relation to cyber attacks on critical infrastructure.

One of the alternatives to exclusive reliance on the ICC is the strengthening of domestic prosecutions[257]. It should also be supported by international cooperation since national courts are often better positioned to investigate and prosecute such cases, particularly where they have access to evidence and technical expertise[258].This is especially true in the context of infrastructure attacks, where the affected systems, victims, and operational impacts are typically located within the territory of one targeted state, just like the earlier illustrated cyber attacks against Ukraine. Domestic authorities are, therefore, uniquely situated to collect digital evidence, interview witnesses, and assess the functional consequences of cyber operations. Ukraine has a specialized Computer Emergency Response Team (hereinafter – CERT-UA) that investigates cyber incidents and warns civilians about cyber activity, just recently, in April of 2026, it has reported that cyber attacks against hospitals and local

[255] Wilmshurst, Elizabeth, Harriet Moynihan, and Tsvetelina van Benthem. *"*Securing Justice for Cyber-Enabled International Crimes: Legal Foundations and Practical Routes to Prosecution*." Chatham House*, (2026): 38.
[256] Ibid, p. 59-64.
[257] Ibid, p. 30-31.
[258] Ibid, p. 56-57.

governmental bodies have intensified[259]. Domestic investigators, such as CERT-UA, therefore have a critical position for creating cyber expertise and evidentiary preservation. Unlike international bodies, which often depend on second-hand submissions or delayed cooperation, national institutions are able to access compromised systems in real time, secure volatile data, and reconstruct the sequence of intrusion through forensic analysis of malware, network traffic, and system logs[260]. And with continues cooperation, such domestic teams can lead investigations that progressively bridge the gap between technical attribution and legal qualification, for example, The State Service of Special Communications and Information Protection of Ukraine has approved a mechanism for delegating tasks from CERT-UA to sectoral and regional Computer Security Incident Response Teams[261]. Such teams operate as specialized incident response units that combine technical capabilities, such as malware analysis, log examination, and real-time threat detection, with coordinated information sharing to prevent, detect, mitigate, and recover from cyber incidents[262]. In the context of infrastructure cyber attacks, their ability to analyze incidents, preserve evidence, and exchange intelligence across national and international networks can increase both the effectiveness of investigations and the reconstruction of broader attack patterns for their legal qualification. Afterall, domestic prosecutions operate within the framework of complementarity, reinforcing rather than replacing the role of international institutions such as the ICC[263]. However, these advantages also come with important limits. It is often difficult to deal with cases where perpetrators operate across borders, and sometimes states may be unwilling to prosecute individuals connected to their own political or strategic interests. In addition, weak coordination between

---

[259] CERT-UA. "Hospitals, Local Government Bodies, and FPV Operators are the Focus of the UAC-0247 (UAC-0244) Cyber Threat Cluster", 20 April 2025. https://cert.gov.ua/article/6288271

[260] Wilmshurst, Elizabeth, Harriet Moynihan, and Tsvetelina van Benthem. *"Securing Justice for Cyber-Enabled International Crimes: Legal Foundations and Practical Routes to Prosecution." Chatham House*, (2026): 38.

[261] State Service of Special Communications and Information Protection of Ukraine (SSSCIP), " SSSCIP Decentralises Cyber Response: CERT-UA to Empower Sectoral and Regional Teams,"April 2026. https://cip.gov.ua/en/news/derzhspeczv-yazku-decentralizuye-reaguvannya-na-kiberzagrozi-cert-ua-deleguvatime-zavdannya-galuzevim-ta-regionalnim-csirt

[262] Pauline Meyer and Sylvain Métille, "Computer Security Incident Response Teams: Are They Legally Regulated? The Swiss Example," *International Cybersecurity Law Review* 4, no. 1 (2023). https://doi.org/10.1365/s43439-022-00070-x.

[263] Oleg Tatarov, "The Principle of Complementarity between International and Domestic Jurisdictions in the Prosecution of War Crimes," *Baltic Journal of Economic Studies* 12, no. 2 (2026): p.105.

different national systems can lead to fragmentation and reduce the overall effectiveness of accountability efforts. Because of this, scholars highlight the need for stronger cooperation, such as joint investigations, shared evidence systems, and collaboration with organizations like Europol, Eurojust and Interpol[264]. This shows a broader shift toward what scholars and practitioners call "networked accountability," where different actors work together as part of one connected investigative process[265].

Closely related to these challenges is the problem of attribution, which remains one of the most significant barriers to accountability in the cyber context, particularly in relation to cyber operations carried out during the Russia–Ukraine war. The establishment of an international attribution mechanism has become as a key proposal within academic and policy discourse[266]. As argued by some international criminal law scholars, the absence of a credible, independent body capable of establishing factual attribution undermines the effective operation of international legal frameworks[267], a challenge that has been repeatedly observed in attempts to attribute cyber attacks against Ukrainian infrastructure. This issue is particularly important in relation to cyber attacks on infrastructure, including incidents affecting Ukrainian energy systems, telecommunications networks such as Kyivstar, and state databases, which are often deliberately designed to hide their origin through techniques such as routing through multiple jurisdictions, deploying false flags, and relying on proxy actors[268].

Therefore, the creation of an international attribution mechanism offers clear advantages in light of existing scholars' works. This is particularly relevant in the context of the Russia-Ukraine war, where cyber operations against critical infrastructure have been widely documented but often remain difficult to attribute conclusively at the international level. In such cases, the absence of a centralized and authoritative attribution mechanism complicates the translation of technical findings

---

[264] Wilmshurst, Elizabeth, Harriet Moynihan, and Tsvetelina van Benthem. *"*Securing Justice for Cyber-Enabled International Crimes: Legal Foundations and Practical Routes to Prosecution*." Chatham House*, (2026).
[265] Patryk Pawlak, "*Accountability in Cyberspace: The Holy Grail of Cyber Stability?*, Policy Brief".EU Cyber Direct (2024): 11-23.
[266] Yuval Shany and Michael N. Schmitt, "An International Attribution Mechanism for Hostile Cyber Operations," *International Law Studies* 96 (2020): 218.
[267] Ibid, 220.
[268] Herbert Lin, "Attribution of Malicious Cyber Incidents," *Journal of International Affairs* 70, no. 1 (2016): 6-7.

into legally reliable evidence for accountability processes, including potential proceedings before the International Criminal Court. As Lin explains, attribution in cyberspace is rarely based on a single decisive piece of evidence, but instead relies on combining multiple technical and contextual clues, none of which are fully conclusive on their own[269]. A centralized and independent body could therefore enhance the credibility and consistency of attribution by standardizing how such evidence is assessed. At the same time, such a mechanism could help bridge the gap between technical findings and legal responsibility. Lin emphasizes that technical forensics alone cannot identify the true perpetrator, and that attribution must extend beyond identifying the individual actor to determining the "ultimately responsible adversary."[270] However, important challenges remain, including political resistance, uncertainty in attribution judgments, and the lack of definitive proof, as attackers can deny involvement or manipulate evidence. Despite this, attribution remains a necessary foundation for accountability especially since international law depends on a reliable factual basis to function.[271]

A more ambitious, though considerably more controversial, proposal involves the creation of a specialized international cyber tribunal. The concept of an International Criminal Tribunal for Cyberspace (ICTC) reflects the perception that existing institutions are insufficient to address the scale, complexity, and transnational nature of cyber operations[272]. As highlighted by Judge Schjolberg in the ICTC proposal, the absence of a dedicated international court risks leaving many serious cyberattacks, particularly those targeting critical infrastructure, unpunished[273]. This argument is connected to the observation that has been mentioned before – cyber operations often transcend national boundaries, involve multiple actors, and produce effects that cannot be adequately addressed within territorially limited legal frameworks. This proposal is also relevant in the context of the Russia-Ukraine war,

[269] Ibid, 24-25.
[270] Ibid, 5-10.
[271] Ibid, 2.
[272] Stein Schjolberg, "An International Criminal Tribunal for Cyberspace (ICTC)", *EastWest Institute Cybercrime Legal Working Gro*up (2012): 3.
[273] Ibid, 3.

where large-scale cyber operations have been carried out involving state-affiliated or proxy actors. In such circumstances, domestic prosecutions face clear limitations, both in terms of jurisdiction and access to evidence, while existing international mechanisms have yet to fully capture the complexity of these operations. As a result, a specialized tribunal could, at least in theory, provide a more coherent framework for addressing cross-border cyber conduct and consolidating fragmented evidence into a single accountability process. The potential advantages of such a tribunal are clear. A specialized institution could develop expertise in cyber law, digital evidence, and technical attribution, thereby enhancing the quality and consistency of prosecutions[274]. Its global jurisdiction would allow it to address cross-border operations more effectively than domestic courts, while its symbolic significance would reinforce the international community's commitment to accountability in cyberspace[275]. However, the likelihood of bringing this proposal to real life remains highly uncertain. The creation of a new international tribunal would require broad political agreement, which is unlikely given the strategic interests of major cyber powers[276]. Additionally, the potential overlap with the ICC raises concerns about jurisdictional fragmentation and institutional duplication, therefore, while the ICTC proposal highlights important structural deficiencies in the current system, it is best understood as a conceptual benchmark rather than an immediate solution.

In light of these limitations, increasing attention has been devoted to hybrid and multi-level accountability models, because these frameworks seek to combine elements of international law, domestic prosecution, technical expertise, and private sector involvement into a more flexible and adaptive system [277]. Effective accountability requires multi-level institutional coordination, involving cooperation between states, international organizations, private companies, and civil society actors [278]. This approach is particularly suitable for cyber operations targeting

[274] Ibid, 9-17.
[275] Ibid, 10.
[276] Franziska Klopfer, *"*Accountability in Cybersecurity"*, Geneva Centre for Security Sector Governance*, (2024): 18.
[277] Wilmshurst, Elizabeth, Harriet Moynihan, and Tsvetelina van Benthem. *"*Securing Justice for Cyber-Enabled International Crimes: Legal Foundations and Practical Routes to Prosecution*." Chatham House*, (2026): 47-49.
[278] Ibid, p. 52.

infrastructure, as these systems are highly interconnected and depend on both public and private networks operating across multiple jurisdictions.

The cross-border nature of cyberspace and the involvement of different types of actors make purely state-centered responses insufficient[279]. Hybrid models therefore offer important advantages. Their flexibility allows them to adapt to the specific characteristics of individual cyber incidents, which can vary significantly in scale, intent, and impact. This adaptability is essential in a domain where threats are constantly evolving. Another key benefit is inclusivity. Because much of critical infrastructure and cyber expertise is concentrated in the private sector, hybrid frameworks make it possible to integrate technical knowledge and operational capabilities that states alone may lack[280]. This improves both the quality of investigations and the overall effectiveness of responses.

At the same time, these models are more practical and politically feasible. Rather than creating entirely new international institutions, they build on existing structures and forms of cooperation, which reduces the need for extensive political agreement and institutional redesign. However, significant challenges remain. Effective coordination in cyberspace is difficult because governance is no longer confined to a single level or actor, but instead operates across intertwined global and local dynamics, as well as public and private spheres. This creates a structurally complex environment in which cooperation depends not only on legal frameworks, but also on sustained political engagement and alignment of interests among diverse stakeholders[281]. At the same time, the distribution of responsibilities across multiple actors contributes to fragmentation, because the traditional model of a unitary state is increasingly replaced by a plurality of institutions and actors that shape norms beyond territorial boundaries. While this reflects the reality of cyberspace, it also risks creating gaps in accountability, as no single actor retains full control or responsibility over cyber operations.

---

[279] Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," International Security 41, no. 3 (2017): 44-71

[280] Ibid, 44-71.

[281] Wilmshurst, Elizabeth, Harriet Moynihan, and Tsvetelina van Benthem. *"*Securing Justice for Cyber-Enabled International Crimes: Legal Foundations and Practical Routes to Prosecution*." Chatham House*, (2026): p. 58.

Moreover, the hybrid nature of cyberspace blurs key distinctions, including those between national and international governance, and between state and non-state actors[282]. This makes coordination more difficult, as different actors operate according to their own priorities, legal frameworks, and strategic interests, often leading to competing approaches rather than unified responses. Nevertheless, hybrid frameworks represent one of the possible responses to these conditions. Rather than attempting to impose centralized control, they acknowledge that cyberspace is inherently shaped by the interaction of technological, political, and social factors, and therefore requires distributed forms of governance[283]. In this sense, hybridity is not a flaw but simply defining feature of the system that differentiates it from others.

In conclusion, the OTP Policy, while essential, might be not enough on its own to ensure accountability for cyber operations, including targeting critical infrastructure. The complexity of such operations requires a layered and multi-dimensional approach, combining domestic prosecutions, international cooperation, attribution mechanisms, and, where appropriate, institutional innovation. Rather than relying on a single solution, effective accountability must emerge from the interaction of multiple frameworks, each addressing specific aspects of the problem. Ultimately, the challenge lies not in redefining the law, but in developing the institutional capacity to apply it effectively in the digital age.

***

One of the key issues of the existing international criminal framework is the lack of a clear and unified understanding of what cybercrime actually is. Different scholars and legal instruments use different terms and definitions, which creates fragmentation and uncertainty: some approaches treat cybercrime as a broad umbrella concept, while others try to narrow it down to specific types of conduct, such as attacks on computer systems. Although distinctions like cyber-dependent and cyber-enabled crimes help to structure the discussion, they still do not fully solve the problem. Instead, they show that cyber conduct is very diverse and cannot be easily placed into one category. This

[282] Joseph S. Nye Jr., "The Regime Complex for Managing Global Cyber Activities," *GCIG Paper Series* No. 1, Centre for International Governance Innovation/Chatham House (2014): 6..
[283] Ibid, 7.

makes it harder to define clear legal thresholds and to decide when certain actions should lead to international criminal responsibility.

Another important limitation is related to the mental element of crimes. Under the Rome Statute, liability depends on intent and knowledge, meaning that a person must be aware of the consequences of their actions, however, in cyber operations, especially those involving complex systems or automated tools, outcomes are not always predictable. Malware can spread beyond its original target, and operations can have indirect or delayed effects. In such situations, it becomes difficult to prove that the perpetrator had the required level of certainty about the consequences. At the same time, expanding the concept of *mens rea* to include recklessness or risk-taking could create new problems, such as lowering the threshold of responsibility or making legal standards less clear. Because of this, the current approach creates a gap where harmful conduct may not meet the strict requirements of intent, even if the risks were foreseeable.

The problem becomes even more complex when looking at how cyber operations are actually carried out. Unlike traditional crimes, which are often committed by clearly structured groups, cyber operations are usually distributed across multiple actors. Different individuals may design, deploy, support, or benefit from an operation, often without direct contact with each other. Some actors may not even fully understand the final outcome of their contribution. This makes it difficult to apply traditional concepts like co-perpetration, joint criminal enterprise, or command responsibility, all of which depend on a certain level of coordination, control, or shared intent. In cyber contexts, these elements are often weak or completely absent. As a result, responsibility becomes diffused across the network, and it is hard to identify a single individual whose role is strong enough to meet the threshold of international criminal liability.

At the same time, interpretive approaches to the Rome Statute show that the law is not completely incapable of dealing with cyber operations. Many scholars argue that there is no need to create a new category of “cybercrime” within international criminal law. Instead, cyber conduct can be assessed under existing crimes, such as war crimes

or crimes against humanity, if it meets the required elements. This idea is supported by the general understanding that the law is technologically neutral, meaning that it does not depend on whether harm is caused through physical or digital means. However, this approach also has its limits. It requires stretching existing legal concepts to fit situations that they were not originally designed for, especially in cases where harm is indirect, cumulative, or primarily affects systems rather than individuals in an immediate way.

The adoption of the OTP Policy on Cyber-Enabled Crimes represents an important step in clarifying how these interpretive approaches should work in practice. The Policy confirms that cyber means can be used to commit existing international crimes and provides guidance on how such conduct should be analyzed. It also introduces useful distinctions, such as between cyber-dependent and cyber-enabled crimes, and emphasizes the importance of looking at the broader context of actions rather than isolated incidents. This is particularly relevant in situations where multiple cyber operations form part of a larger campaign, for example, targeting civilian infrastructure. At the same time, the Policy does not solve all problems. It does not change the law itself and does not remove the practical difficulties related to evidence, attribution, and enforcement.

Cyber attacks on Ukrainian infrastructure clearly illustrate both the possibilities and the limits of the current framework. Cyber operations targeting energy systems, communication networks, and state databases show that non-kinetic actions can have very real consequences for civilian populations. Disruptions to electricity, especially during winter, can affect heating, healthcare, and access to basic services. When such operations are repeated and combined with other forms of attack, they may form part of a broader pattern that could be relevant for international criminal law. At the same time, even in such well-documented situations, proving individual responsibility remains extremely difficult. Technical evidence exists, but linking it to specific individuals and meeting the required legal standards is still a major challenge.

Because of these limitations, it becomes clear that relying only on international criminal law, even with the support of interpretive tools like the OTP Policy, is not

enough and that accountability for cyber operations requires a broader approach that includes multiple levels and actors. Domestic prosecutions can play an important role, especially in cases where states have direct access to evidence and technical expertise, but international cooperation is also essential, as cyber operations often cross borders and involve actors from different jurisdictions. In addition, proposals such as international attribution mechanisms or even specialized tribunals reflect the need to address gaps that cannot be solved within the existing system alone. Hybrid and multi-level models appear to offer the most realistic way forward, because these approaches combine legal, technical, and institutional elements, allowing different actors to contribute to the process of accountability, and they also reflect the nature of cyberspace itself, which is not controlled by a single actor but shaped by interactions between states, private companies, and other stakeholders. However, they also create new challenges, especially in terms of coordination and distribution of responsibility, since when many actors are involved, it becomes harder to ensure consistency and to avoid gaps in accountability.

Overall, the main difficulty lies not in the absence of legal norms, but in the gap between legal qualification and practical enforcement. Cyber operations expose the limits of a system that is based on clear structures, direct causation, and individual intent. While the law can be interpreted to include many forms of cyber conduct, turning that interpretation into effective accountability remains a complex and unresolved issue. This suggests that future developments should focus not only on legal interpretation, but also on building institutional and practical capacity to deal with the specific challenges of the digital environment, until then accountability for cyber operations will likely remain partial and uneven, depending not only on the strength of legal frameworks but also on the availability of technical expertise, political will, and effective cooperation between different actors.

CONCLUSIONS

The transformation of armed conflict in the digital era demonstrates that international law is no longer applied in a stable and, to some degree, predictable environment, but in a constantly evolving space where traditional categories are increasingly difficult to maintain. As the research within the thesis has shown, cyber operations challenge not only the technical understanding of conflict, but also the legal frameworks that were designed to regulate it. While existing regimes, including international humanitarian law, international human rights law, and international criminal law, formally remain applicable, their ability to provide effective accountability in practice is significantly limited.

The analysis of cyber warfare as a domain has confirmed that its defining characteristics, such as anonymity, lack of clear boundaries, and the involvement of both state and non-state actors, fundamentally complicate the application of *jus ad bellum*. The absence of a unified definition of cyber warfare, combined with the lack of consensus on thresholds for the use of force, creates a legal environment where similar operations may be interpreted differently depending on the approach applied. Effects-based, target-based, and character-based interpretations each offer partial solutions, yet none of them fully captures the complexity of cyber operations. As a result, states hold significant discretion in qualifying cyber conduct under their national norms, which increases the risk of both under-regulation and escalation.

At the same time, the problem of attribution remains one of the most significant practical barriers to accountability. Even where harmful cyber operations can be identified, linking them to a specific state, or even group, under existing standards of control is often difficult. The divergence between the effective control and overall control tests further illustrates the lack of coherence in this area. Although alternative approaches, such as due diligence or hybrid attribution models, offer promising directions, they remain insufficiently developed and inconsistently applied. This creates a situation in which states may exploit technological anonymity to avoid responsibility, at the same time weakening the core functions of international law.

From the perspective of human rights, the research has demonstrated that the digital environment exposes structural limitations within the traditional framework. The concept of “violation error” illustrates how certain interferences with rights may remain unrecognized due to their non-kinetic and systemic nature. Cyber operations targeting critical infrastructure, in particular, reveal that harm is often indirect, cumulative, and delayed, making it difficult to assess within existing legal categories. While the extension of offline rights to the online sphere remains an important starting point, it is not always sufficient to address the specific risks posed by digital technologies. This suggests a need not only for reinterpretation, but also for a more flexible understanding of harm within human rights law.

The limitations become even more visible within international criminal law. As the research has shown, the current framework of the Rome Statute was not designed with cyber operations in mind, and its application in this context is constrained by high thresholds of harm, difficulties in establishing intent, and challenges related to modes of liability. The decentralized nature of cyber operations, where multiple actors may contribute to a harmful outcome without a clear hierarchy, complicates the attribution of individual criminal responsibility. Although recent developments, including the Office of the Prosecutor’s Policy on Cyber-Enabled Crimes, represent an important step toward adapting the existing framework, they do not fully resolve these structural issues.

At the same time, the practical analysis of cyber operations against Ukrainian critical infrastructure highlights that these legal limitations are not merely theoretical. The scale and impact of such operations demonstrate that cyber attacks are capable of producing consequences comparable to traditional forms of warfare, yet, the mechanisms for ensuring accountability remain fragmented and often ineffective. This gap between the scale of harm and the availability of legal responses reinforces the need for further development of both doctrinal and institutional approaches.

Considering these findings, several practical and theoretical recommendations can be identified. First, there is a need to further develop interpretative approaches within existing legal frameworks, particularly by expanding the understanding of harm

to include non-physical and systemic effects. Second, greater consistency is required in the application of attribution standards, potentially through the development of hybrid models or international mechanisms capable of assessing technical evidence in a more structured way. Third, institutional innovation, including the strengthening of cooperation between states, international organizations, and private actors, may offer a more realistic pathway toward accountability in complex cyber environments. Finally, continued development of international criminal law, whether through interpretation or more gradual normative evolution, remains essential to address the challenges of individual responsibility in cyberspace.

The research done within the thesis shows that international law is not outdated when it comes to cyber warfare, but it is clearly under serious pressure. Its existing structures provide a foundation, yet they require careful adaptation to remain effective. The challenge lies not just in choosing between entirely new rules and the strict application of existing ones, but also in finding a balance between stability and flexibility. The digitalization of conflict has exposed the limits of traditional legal thinking, but it has also created an opportunity for the legal community to rethink how accountability should function in a more interconnected and technologically advanced world. The question that remains is not whether international law applies to cyber warfare, but whether it can evolve quickly enough to ensure that accountability in this domain is more than only theoretical.

LIST OF REFERENCES

1. Abrusci, Elena, and Richard Mackenzie-Gray Scott. “The Questionable Necessity of a New Human Right against Being Subject to Automated Decision-Making.” *International Journal of Law and Information Technology* 31, no. 2 (Summer 2023): 114. https://academic.oup.com/ijlit/article/31/2/114/7227602.
2. Ambos, Kai. “Cyber-Attacks as International Crimes under the Rome Statute of the International Criminal Court?” *ICC Forum*, 7 March 2022. https://iccforum.com/cyberwar#Ambos.
3. Ambos, Kai. “Amending the Rome Statute to Cover Cyberwarfare as Aggression.” *ICC Forum*, UCLA School of Law Promise Institute, March–July 2022. https://iccforum.com/cyberwar.
4. Ambos, Kai. “International Criminal Responsibility in Cyberspace.” In *Research Handbook on Cyberspace and International Law*, edited by N. Tsagourias and R. Buchan, 118–143. Edward Elgar Publishing, 2015. https://ssrn.com/abstract=2412626.
5. Artemchuk, Oleksii. “Number of Cyberattacks on Ukraine Increased by 70% in Past Year.” *Ukrainska Pravda*, 9 January 2025. https://www.pravda.com.ua/eng/news/2025/01/09/7492671/.
6. CERT-UA. “Cyberattack by Sandworm Group (UAC-0082) on Energy Facilities of Ukraine Using Malicious Programs INDUSTROYER2 and CADDYWIPER.” CERT-UA#4435. 12 April 2022. https://cert.gov.ua/article/39518.
7. CERT-UA. “Hospitals, Local Government Bodies, and FPV Operators are the Focus of the UAC-0247 (UAC-0244) Cyber Threat Cluster.” 20 April 2025. https://cert.gov.ua/article/6288271.
8. *Charter of the United Nations*. Signed 26 June 1945. Entered into force 24 October 1945. https://www.un.org/en/about-us/un-charter/full-text.

9. Chengeta, Thompson. “Accountability Gap, Autonomous Weapon Systems and Modes of Responsibility in International Law.” Harvard Law School, 2015. http://dx.doi.org/10.2139/ssrn.2755211.
10. Chwe, Hanyu. “The Rise of Cyber Warfare: The Digital Age and American Decline.” *Swarthmore International Relations Journal* 1, no. 1 (2016). https://doi.org/10.24968/2574-0113.1.11.
11. Civil Society Alliances for Digital Empowerment. “International Criminal Court Issues Policy Clarifying Treatment of Cyber-Enabled Crimes under the Rome Statute.” *CADE Project*, 10 December 2025. https://cadeproject.org/updates/international-criminal-court-issues-policy-clarifying-treatment-of-cyber-enabled-crimes-under-the-rome-statute/.
12. Clark, Roger S. “The Mental Element in International Criminal Law: The Rome Statute of the International Criminal Court and the Elements of Offences.” *Criminal Law Forum* 12 (2001): 291–334. https://doi.org/10.1023/A:1014929127650.
13. Coccoli, Jacopo. “The Challenges of New Technologies in the Implementation of Human Rights: An Analysis of Some Critical Issues in the Digital Era.” *Peace Human Rights Governance* 1, no. 2 (July 2017): 224. https://phrg.padovauniversitypress.it/system/files/papers/2017_2_4.pdf.
14. Collier, Roger. “NHS Ransomware Attack Spreads Worldwide.” *CMAJ* 189, no. 22 (5 June 2017). https://pmc.ncbi.nlm.nih.gov/articles/PMC5461132/.
15. Committee on Economic, Social and Cultural Rights. *General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12)*. UN Doc. E/C.12/2000/4. 11 August 2000. https://www.ohchr.org/sites/default/files/Documents/Issues/Women/WRGS/Health/GC14.pdf.
16. Committee on Economic, Social and Cultural Rights. *General Comment No. 4: The Right to Adequate Housing (Art. 11(1) of the Covenant)*. UN Doc. E/1992/23. 13 December 1991. https://www.refworld.org/legal/general/cescr/1991/53157.

17. Connell, Michael, and Sarah Vogler. *Russia's Approach to Cyber Warfare*. CNA Occasional Paper DOP-2016-U-014231-1Rev. Center for Naval Analyses, 2017. https://apps.dtic.mil/sti/pdfs/AD1032208.pdf.

18. *Convention on Cybercrime*. Opened for signature 23 November 2001. Entered into force 1 July 2004. European Treaty Series No. 185. Council of Europe. https://rm.coe.int/1680081561.

19. Council of Europe. *Explanatory Report to the Convention on Cybercrime*. European Treaty Series No. 185. Budapest, 23 November 2001. https://rm.coe.int/16800cce5b.

20. "Critychna infrastruktura pid prytsilom: yak Ukraina vybudovuye kiberstiykist i choho svit mozhe v nas povchytys'" ["Critical Infrastructure under Fire: How Ukraine Builds Cyber Resilience and What the World Can Learn"]. *Hromadske*, 2025. https://hromadske.ua/specials/254318-krytychna-infrastruktura-pid-prytsilom-iak-ukrayina-vybudovuye-kiberstiykist-i-choho-svit-moze-v-nas-povchytys.

21. "Cyberwarfare Issue: When Might Cyber Operations Constitute Crimes Under the Rome Statute?" *ICC Forum*, UCLA School of Law Promise Institute, March–July 2022. https://iccforum.com/cyberwar.

22. De Colle, Giacomo. "Towards an Ontology of State Actors in Cyberspace." *Cornell University*, 2024. https://arxiv.org/pdf/2408.01787.

23. De Tomas Colatin, Samuele. "Power Grid Cyberattack in Ukraine (2015)." *International Cyber Law: Interactive Toolkit*. NATO Cooperative Cyber Defence Centre of Excellence. https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015).

24. Defence Intelligence of Ukraine. "Invaders Preparing Mass Cyberattacks on Facilities of Critical Infrastructure of Ukraine and Its Allies." 26 September 2022. https://gur.gov.ua/en/content/okupanty-hotuiut-masovani-kiberataky-na-ob-iekty-krytychnoi-infrastruktury-ukrainy-ta-ii-soiuznykiv.html.

25. Denny, Eric J. "The Cyberspace Domain: Path to a New Service?" Monograph, School of Advanced Military Studies, US Army Command and General Staff

College, 2013. https://nsarchive.gwu.edu/sites/default/files/documents/2917523/Document-05.pdf.

26. DiploFoundation. "International Criminal Court (ICC) Issues Policy on Cyber-Enabled Crimes." *Digital Watch Observatory*. 13 December 2025. https://dig.watch/updates/international-criminal-court-icc-issues-policy-on-cyber-enabled-crimes.
27. Dror-Shpoliansky, Dafna, and Yuval Shany. "It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology." *European Journal of International Law* 32, no. 4 (2021): 1257. https://www.ejil.org/pdfs/32/4/3208.pdf.
28. Dysa, Yuliia. "Ukraine Says Russian Cyberattack Hits State Registries but No Data Lost." *Reuters*, 20 December 2024. https://www.reuters.com/technology/cybersecurity/ukraine-says-russian-cyberattack-hits-state-registries-no-data-lost-2024-12-20/.
29. European Court of Human Rights. *Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence*. https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng.
30. European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape for Ransomware Attacks*. 2022. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Ransomware%20Attacks.pdf.
31. Finlay, Lorraine, and Christian Payne. "The Attribution Problem and Cyber Armed Attacks." *AJIL Unbound* 113 (2019): 202. https://researchonline.nd.edu.au/cgi/viewcontent.cgi?article=1089&context=law_article.
32. "Géopolitychna sytuatsiia zminylas': Yak Rosiia povnistyu zaboroniaie ukrainsku movu v shkolakh okupovanykh rehioniv" ["The Geopolitical Situation Has Changed: How Russia Is Completely Banning the Ukrainian

Language in Schools in Occupied Regions"]. *BBC News Ukraina*, 26 June 2025. https://www.bbc.com/ukrainian/articles/cev0en0wnlpo.

33. Greipl, Anna Rosalie. "Data-Driven Learning Systems and the Commission of International Crimes: Concerns for Criminal Responsibility?" *Journal of International Criminal Justice* 21, no. 5 (November 2023): 1097. https://academic.oup.com/jicj/article/21/5/1097/7259630.
34. Guilfoyle, Douglas. "Responsibility for Collective Atrocities: Fair Labelling and Approaches to Commission in International Criminal Law." *Current Legal Problems* 64, no. 1 (2011): 255–286. https://doi.org/10.1093/clp/cur006.
35. Haataja, Samuli, and Afshin Akhtar-Khavari. "Stuxnet and International Law on the Use of Force: An Informational Approach." *Cambridge International Law Journal* 7, no. 1 (2018): 3. https://research-repository.griffith.edu.au/server/api/core/bitstreams/b5540c24-8492-4f45-9e9e-90781a5de185/content.
36. Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack." *California Law Review* 100, no. 4 (2012): 817–885. https://www.researchgate.net/publication/251334352_The_Law_of_Cyber-Attack.
37. Hayat, Zia. "Digital Trust: How to Unleash the Trillion-Dollar Opportunity for Our Global Economy." World Economic Forum, 2022. https://www.weforum.org/stories/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/.
38. He, Thomas, and Ying Yu Lin. "Cyberspace Force Equipment at the 2025 Military Parade." *China Brief Notes*. Jamestown Foundation, 10 January 2025. https://jamestown.org/cyberspace-force-equipment-at-the-2025-military-parade/.
39. Human Rights Committee. *General Comment No. 36: Article 6 (Right to Life)*. UN Doc. CCPR/C/GC/36. 3 September 2019. https://documents.un.org/doc/undoc/gen/g19/261/15/pdf/g1926115.pdf.

40. Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." *Leading Issues in Information Warfare & Security Research* 1 (2011): 1–14. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

41. ICC Office of the Prosecutor. *Policy on Cyber-Enabled Crimes under the Rome Statute*. ICC, December 2025. https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf.

42. ICC OTP Issues First Policy on Cyber-Enabled Crimes." *International Law in Brief*. American Society of International Law, 13 January 2026. https://asil.org/ilib/icc-otp-issues-first-policy-cyber-enabled-crimes/.

43. International Committee of the Red Cross. "Commentary on Article 33." In *Convention (IV) Relative to the Protection of Civilian Persons in Time of War of 12 August 1949: Commentary of 2025*. https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-33/commentary/2025.

44. International Committee of the Red Cross. "Cyber Operations during Armed Conflict: The Principle of Proportionality." Fact sheet. Geneva: ICRC, March 2023. https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/04_proportionality-0.pdf.

45. International Committee of the Red Cross. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Building a Culture of Compliance for IHL to Protect Humanity in Today's and Future Conflicts*. ICRC, October 2024. https://www.icrc.org/en/publication/international-humanitarian-law-and-challenges-contemporary-armed-conflicts-building.

46. International Committee of the Red Cross. *International Humanitarian Law and Cyber Operations during Armed Conflicts*. ICRC Position Paper. ICRC, November 2019. https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf.

47. International Committee of the Red Cross. "Views of the International Committee of the Red Cross (ICRC) on Autonomous Weapon Systems." Background paper submitted to the CCW Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Geneva, 2016. https://www.icrc.org/en/document/views-icrc-autonomous-weapon-system.

48. International Court of Justice. *Legality of the Threat or Use of Nuclear Weapons*. Advisory Opinion. I.C.J. Reports 1996, p. 226. 8 July 1996. https://iilj.org/wp-content/uploads/2016/08/Legality-of-the-Threat-or-Use-of-Nuclear-Weapons-1996.pdf.

49. International Court of Justice. "Situation in Ukraine: ICC Judges Issue Arrest Warrants against Sergei Kuzhugetovich Shoigu and Valery Vasilyevich Gerasimov." 5 September 2024. https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-sergei-kuzhugetovich-shoigu-and.

50. International Court of Justice, Office of the Prosecutor. "Questions and Answers: The ICC Office of the Prosecutor's Policy on Cyber-Enabled Crimes under the Rome Statute." 3 December 2025. https://www.icc-cpi.int/about/otp/questions-and-answers-the-icc-office-of-the-prosecutors-policy-on-cyber-enabled-crimes-under-the-rome-statute.

51. *International Covenant on Civil and Political Rights*. Adopted 16 December 1966. Entered into force 23 March 1976. 999 UNTS 171. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

52. International Law Commission. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*. 2001. UN Doc. A/56/10. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

53. International Telecommunication Union. *ITU Council 2010 Highlights* No. 3. 2010. https://www.itu.int/council/C2010/pd/highlights/apr15.html.

54. Institute of Mass Information. "Russia's Crimes against the Media: At Least 100 Cyber Attacks on the Media and Journalists in the 3 Years since the Start of the Invasion." *IMI*, 21 February 2025. https://imi.org.ua/en/news/russia-s-crimes-

against-the-media-at-least-100-cyber-attacks-on-the-media-and-journalists-in-the-3-i66765.

55. Jenks, Chris. "Motive Matters: The Meaning of Attack Under IHL & the Rome Statute." *Opinio Juris*, 26 October 2020. http://opiniojuris.org/2020/10/26/motive-matters-the-meaning-of-attack-under-ihl-the-rome-statute/.

56. Jiang, Zhifeng. "Regulating the Use and Conduct of Cyber Operations through International Law: Challenges and Fact-Finding Body Proposal." *LSE Law Review* 5 (2020): 63. https://lawreview.lse.ac.uk/articles/42/files/submission/proof/42-1-90-3-10-20200318.pdf.

57. Klopfer, Franziska. *Accountability in Cybersecurity*. Geneva Centre for Security Sector Governance, 2024. https://www.dcaf.ch/sites/default/files/publications/documents/accountability-cybersecurity.pdf.

58. Kulesza, Joanna. "ICC Cyber-Enabled Crimes and DNS Abuse: Accountability Questions for Infrastructure Operators." *CircleID*, 18 December 2025. https://circleid.com/posts/icc-cyber-enabled-crimes-and-dns-abuse-accountability-questions-for-infrastructure-operators.

59. Lee, Robert M., Michael J. Assante, and Tim Conway. *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*. E-ISAC/SANS, 18 March 2016. https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf.

60. *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970)*. Advisory Opinion. I.C.J. Reports 1971, p. 16. https://www.icj-cij.org/case/53.

61. Lemnitzer, Jan Martin. "Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace." *European Journal of International Law* 33, no. 3 (2022): 794–795. https://www.ejil.org/pdfs/33/3/3288.pdf.

62. Li, Yuchong, and Qinghui Liu. "A Comprehensive Review Study of Cyber-Attacks and Cyber Security: Emerging Trends and Recent Developments." *Energy Reports* 7 (November 2021): 8177. https://www.sciencedirect.com/science/article/pii/S2352484721007289.

63. Lin, Herbert. "Attribution of Malicious Cyber Incidents." *Journal of International Affairs* 70, no. 1 (2016): 6–7. https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.

64. Lohmann, Sarah J., et al. *What Ukraine Taught NATO about Hybrid Warfare*. US Army War College Press, 2022. https://press.armywarcollege.edu/monographs/956/.

65. Lusthaus, Jonathan. "Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?" *Annual Review of Law and Social Science* 20 (2024): 369. https://www.annualreviews.org/content/journals/10.1146/annurev-lawsocsci-041822-044042.

66. Mačak, Kubo. "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law." *Israel Law Review* 48, no. 1 (2015): 56–59. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2456955.

67. Mahmudov, Nuran. "Cyber Warfare: Understanding the Elements, Effects, and Future Trends of Cyber-Attacks and Defences." *Security & Defense*, no. 2 (2023): 38. https://institute.nvu.bg/sites/default/files/inline-files/2023-2-03-mahmudov.pdf.

68. Matos, Luís. "Cyberattacks as Crimes Against Humanity and International Responsibility of States." 2021. http://dx.doi.org/10.2139/ssrn.3953744.

69. McGuire, Mike, and Samantha Dowling. *Cyber Crime: A Review of the Evidence*. Home Office Research Report 75. Chapter 1: Cyber-Dependent Crimes. London: Home Office, October 2013.

https://assets.publishing.service.gov.uk/media/5a7c83c1ed915d48c241043f/horr75-chap1.pdf.

70. McGuire, Mike, and Samantha Dowling. *Cyber Crime: A Review of the Evidence*. Home Office Research Report 75. Chapter 2: Cyber-Enabled Crimes — Fraud and Theft. London: Home Office, October 2013. https://assets.publishing.service.gov.uk/media/5a755a94e5274a59fa7177f7/horr75-chap2.pdf.

71. Mehta, Devanshi. "Cyber-Enabled International Crimes and the Fragmentation of Jurisdictional Frameworks: Examining the ICC's 2025 Policy in the Context of Cross-Border Digital Warfare." *Record of Law*, 31 March 2026. https://recordoflaw.in/cyber-enabled-international-crimes-and-the-fragmentation-of-jurisdictional-frameworks-examining-the-iccs-2025-policy-in-the-context-of-cross-border-digital-warfare/.

72. Meyer, Pauline, and Sylvain Métille. "Computer Security Incident Response Teams: Are They Legally Regulated? The Swiss Example." *International Cybersecurity Law Review* 4, no. 1 (2023). https://doi.org/10.1365/s43439-022-00070-x.

73. Milanovic, Marko. "ICC Office of the Prosecutor Releases Draft Policy on Cyber-Enabled Crimes." *EJIL: Talk!*, 4 April 2025. https://www.ejiltalk.org/icc-office-of-the-prosecutor-releases-draft-policy-on-cyber-enabled-crimes/.

74. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. Merits, Judgment. I.C.J. Reports 1986. https://www.icj-cij.org/case/70.

75. Miller, Kevin L. "The Kampala Compromise and Cyberattacks: Can There Be an International Crime of Cyber-Aggression?" *Southern California Interdisciplinary Law Journal* 23 (2014): 217–260. https://gould.usc.edu/wp-content/uploads/legacy/why/students/orgs/ilj/assets/docs/6%20-%20Miller.pdf.

76. MITRE ATT&CK. "2015 Ukraine Electric Power Attack." Campaign C0028. 2024. https://attack.mitre.org/campaigns/C0028/.

77. “Modbus Vulnerabilities Used for Cyberattack on a Heating Utility.” *Veridify Security*, 26 July 2024. https://www.veridify.com/article/modbus-vulnerabilities-used-for-cyberattack-on-a-heating-utility/.

78. Moynihan, Harriet. “Securing Justice for Cyber-Enabled International Crimes.” *Just Security*, 3 February 2026. https://www.justsecurity.org/129752/justice-cyber-international-crimes/.

79. Mugari, Evans. “Kyivstar Cyber Attack: A Deep Dive into Cyber Warfare in Ukraine.” *SIGNAL Media* (AFCEA International), July 2025. https://www.afcea.org/signal-media/cyber-edge/kyivstar-cyber-attack-deep-dive-cyber-warfare-ukraine.

80. Muzyka, V. V. “Analiz kiberatak proty system enerhozabezpechennia Ukrainy v konteksti konfliktu na Donbasi” [Analysis of Cyber-Attacks on Ukrainian Power Grid Systems in the Context of Armed Conflict in Donbas]. *Pravova Derzhava*, vyp. 39 (2020): 79. https://www.researchgate.net/publication/346745451.

81. NATO Cooperative Cyber Defence Centre of Excellence. “Scenario 34: Crimes against Humanity.” *International Cyber Law: Interactive Toolkit*. https://cyberlaw.ccdcoe.org/wiki/Scenario_34:_Crimes_against_humanity.

82. Ninan, Johan, Bharadwaj R. K. Mantha, and Balaji Kesavan. “Human-Centred Cybersecurity for Critical Infrastructure: The Case of the Florida Water Plant Hack.” *Engineering, Construction and Architectural Management* 32, no. 13 (2025): 547. https://www.emerald.com/ecam/article-pdf/32/13/547/11041598/ecam-02-2025-0213en.pdf.

83. North Atlantic Treaty Organization. “Cyber Defence.” 2024. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence.

84. Nurse, Jason R. C., and Maria Bada. “The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations.” In *The Oxford Handbook of Cyberpsychology*. Oxford University Press, 2019. https://doi.org/10.1093/oxfordhb/9780198812746.013.36.

85. Nye, Joseph S., Jr. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (Winter 2016/17): 44-71. https://doi.org/10.1162/ISEC_a_00266.

86. Nye, Joseph S., Jr. “The Regime Complex for Managing Global Cyber Activities.” *GCIG Paper Series* No. 1. Centre for International Governance Innovation/Chatham House, 2014. https://www.cigionline.org/static/documents/gcig_paper_no1.pdf.

87. Ohlin, Jens David. “Did Russian Cyber Interference in the 2016 Election Violate International Law?” *Texas Law Review* 95 (2017): 1579. https://scholarship.law.cornell.edu/facpub/1498/.

88. Ophardt, Jonathan A. “Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow’s Battlefield.” *Duke Law & Technology Review* 9 (2010). https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1198&context=dltr.

89. “Oxford English Dictionary.” Under “warfare, n.” https://www.oed.com/dictionary/warfare_n.

90. Pajuste, Tiina. “Adapting Human Rights to a Digital World.” In *Human Rights in the Digital Domain: Core Questions*, edited by Tiina Pajuste. Cambridge University Press, 2025. https://www.cambridge.org/core/books/human-rights-in-the-digital-domain/adapting-human-rights-to-a-digital-world/E2D243C1BCFE8F499622AF31EF975424.

91. Paskevych, Anna [Анна Паскевич]. “U SBU rozkryly, khto stoit za kiberatakoyu na derzhreestry Ukrainy y chy mih statysia vytik danykh” [The SBU Revealed Who Is Behind the Cyberattack on Ukraine’s State Registries and Whether a Data Leak Could Have Occurred]. *Obozrevatel*, 20 December 2024. https://news.obozrevatel.com/ukr/society/u-sbu-rozkrili-hto-stoit-za-kiberatakoyu-na-derzhreestri-ukraini-j-chi-mig-statisya-vitik-danih.htm.

92. Pawlak, Patryk. *Accountability in Cyberspace: The Holy Grail of Cyber Stability?* Policy Brief. EU Cyber Direct, March 2024.

https://www.universiteitleiden.nl/binaries/content/assets/governance-and-global-affairs/isga/accountability-in-cyberspace-patryk-pawlak-march-2024.pdf.

93. Permanent Mission of Liechtenstein to the United Nations. *The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare*. Global Institute for the Prevention of Aggression, August 2021. https://crimeofaggression.info/wp-content/uploads/GIPA_The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf.
94. Phillips, Kirsty, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken. "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies." *Forensic Sciences* 2, no. 2 (2022): 379. https://doi.org/10.3390/forensicsci2020028.
95. Pobjie, Erin. "The Meaning of Prohibited 'Use of Force' in Article 2(4) of the UN Charter." *Articles of War*. Lieber Institute West Point, 2024. https://lieber.westpoint.edu/meaning-prohibited-use-force-article-24-un-charter/.
96. Pollard, Miles. "A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States." *Pepperdine Policy Review* 16, no. 1 (2024): 6–15. https://digitalcommons.pepperdine.edu/cgi/viewcontent.cgi?article=1216&context=ppr.
97. *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)*. Opened for signature 8 June 1977. Entered into force 7 December 1978. 1125 UNTS 3. https://ihl-databases.icrc.org/en/ihl-treaties/api-1977.
98. *Prosecutor v. Duškŏ Tadić*. Case No. IT-94-1-A. Judgment. ICTY Appeals Chamber. 15 July 1999. https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf.

99. *Prosecutor v. Zejnil Delalić, Zdravko Mučić, Hazim Delić and Esad Landžo (Celebici)*. Case No. IT-96-21-T. Trial Chamber Judgment. ICTY, 16 November 1998. https://www.icty.org/x/cases/mucic/tjug/en/.

100. *Prosecutor v. Thomas Lubanga Dyilo*. Case No. ICC-01/04-01/06. Trial Chamber I. Judgment pursuant to Article 74 of the Statute. ICC, 14 March 2012. https://www.worldcourts.com/icc/eng/decisions/2012.03.14_Prosecutor_v_Lubanga1.pdf.

101. Reich, Pauline C., Stuart Weinstein, Charles Wild, and Allan S. Cabanlong. "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity." *European Journal of Law and Technology* 1, no. 2 (2010). https://ejlt.org/index.php/ejlt/article/view/40.

102. Rodriguez Vidal, Eva. "The Seven Phases of a Cyberattack: A Detailed Look at the Cyber Kill Chain." *Sngular Insights*, 26 March 2025. https://www.sngular.com/insights/360/the-seven-phases-of-a-cyberattack-a-detailed-look-at-the-cyber-kill-chain.

103. *Rome Statute of the International Criminal Court*. Adopted 17 July 1998. Entered into force 1 July 2002. 2187 UNTS 90. https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf.

104. Roscini, Marco. "Cyber Operations as a Use of Force." In *Research Handbook on International Law and Cyberspace*, edited by Nicholas Tsagourias and Russell Buchan. Edward Elgar Publishing, 2015. https://ideas.repec.org/h/elg/eechap/15436_11.html.

105. Roscini, Marco. *Cyber Operations and the Use of Force in International Law*. Oxford University Press, 2014. https://unidel.edu.ng/focelibrary/books/Cyber%20Operations%20and%20the%20Use%20of%20Force%20in%20International%20Law%20by%20Marco%20Roscini%20(z-lib.org)%20(1).pdf.

106. Roscini, Marco. "Gravity in the Statute of the International Criminal Court and Cyber Conduct That Constitutes, Instigates or Facilitates International

Crimes." *Criminal Law Forum* 30 (2019): 247–272. https://ssrn.com/abstract=3435439.

107. Roscini, Marco. "Cyber Operations Can Constitute War Crimes Under the ICC Jurisdiction Without Need to Amend the Rome Statute." *ICC Forum*, UCLA School of Law Promise Institute, March–July 2022. https://iccforum.com/cyberwar.

108. Schabas, William A. *The International Criminal Court: A Commentary on the Rome Statute*. 2nd ed. Oxford University Press, 2016. https://academic.oup.com/oxford-law-pro/book/57464.

109. Scheffer, David. "The Missing Pieces in Article 8 *bis* (Aggression) of the Rome Statute." *Harvard International Law Journal* 58, Online Journal (2017): 84. https://journals.law.harvard.edu/ilj/wp-content/uploads/sites/84/Scheffer-Formatted.pdf.

110. Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Columbia Journal of Transnational Law* 37 (1999): 885–937. https://nsarchive.gwu.edu/sites/default/files/documents/3460881/Document-04-Michael-N-Schmitt-United-States-Air.pdf.

111. Schmitt, Michael N. "Cyber Operations and the *Jus Ad Bellum* Revisited." *Villanova Law Review* 56, no. 3 (2011): 569–605. https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?httpsredir=1&article=1019&context=vlr.

112. Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge University Press, 2017. https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017_.pdf.

113. Schjolberg, Stein. “An International Criminal Tribunal for Cyberspace (ICTC).” *EastWest Institute Cybercrime Legal Working Group*, 2012. https://www.cybercrimelaw.net/documents/ICTC.pdf.

114. Shackelford, Scott J. “State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem.” In *Proceedings of the 2010 Conference on Cyber Conflict*, edited by C. Czosseck and K. Podins. CCD COE Publications, 2010. https://ccdcoe.org/uploads/2018/10/Shackelford-State-Responsibility-for-Cyber-Attacks-Competing-Standards-for-a-Growing-Problem.pdf.

115. Shany, Yuval. “Digital Rights and the Outer Limits of International Human Rights Law.” *German Law Journal* (forthcoming). Hebrew University of Jerusalem Legal Research Paper No. 23-2, October 2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4270794.

116. Shany, Yuval, and Michael N. Schmitt. “An International Attribution Mechanism for Hostile Cyber Operations.” *International Law Studies* 96 (2020). https://digital-commons.usnwc.edu/ils/vol96/iss1/8/.

117. Sharma, Ritwik. “Ecocide as the Fifth International Crime: Is the Rome Statute Compatible with Ecocide?” *Völkerrechtsblog*, 16 January 2025. https://voelkerrechtsblog.org/ecocide-as-the-fifth-international-crime/.

118. Sigholm, Johan. “Non-State Actors in Cyberspace Operations.” *Journal of Military Studies* 4 (2013): 1–36. https://www.researchgate.net/publication/310827486_Non-State_Actors_in_Cyberspace_Operations.

119. Slowik, Joe. *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack*. Dragos, Inc., 15 August 2019. https://pylos.co/wp-content/uploads/2021/02/crashoverride.pdf.

120. Songip, A.R., et al. “Cyberspace: The Warfare Domain.” *World Applied Sciences Journal* 21, no. 1 (2013): 1–8. http://www.idosi.org/wasj/wasj21(1)13/1.pdf.

121. State Service of Special Communications and Information Protection of Ukraine (SSSCIP). “SSCSIP Decentralises Cyber Response: CERT-UA to

Empower Sectoral and Regional Teams." April 2026. https://cip.gov.ua/en/news/derzhspeczv-yazku-decentralizuye-reaguvannya-na-kiberzagrozi-cert-ua-deleguvatime-zavdannya-galuzevim-ta-regionalnim-csirt.

122. Tatarov, Oleg. "The Principle of Complementarity between International and Domestic Jurisdictions in the Prosecution of War Crimes." *Baltic Journal of Economic Studies* 12, no. 2 (2026): 105–115. https://doi.org/10.30525/2256-0742/2026-12-2-105-115.

123. Tikk, Eneken, Kadri Kaska, and Liis Vihul. *International Cyber Incidents: Legal Considerations*. NATO Cooperative Cyber Defence Centre of Excellence, 2010. https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf.

124. Titcomb, James. "Ukrainian Blackout Blamed on Cyber-Attack in World First." *The Daily Telegraph*, 5 January 2016. https://www.telegraph.co.uk/technology/news/12082758/Ukrainian-blackout-blamed-on-cyber-attack-in-world-first.html.

125. Triffterer, Otto, and Kai Ambos, eds. *The Rome Statute of the International Criminal Court: A Commentary*. 3rd ed. C.H. Beck/Hart/Nomos, 2016. https://www.department-ambos.uni-goettingen.de/data/documents/Veroeffentlichungen/Triffterer_Ambos_Rome_Statute_Commentary_3rd_ed_2016.pdf.

126. Tsagourias, Nicholas. "Cyber Attacks, Self-Defence and the Problem of Attribution." *Journal of Conflict and Security Law* 17, no. 2 (Summer 2012): 229–244. https://doi.org/10.1093/jcsl/krs019.

127. UN Human Rights Council. *New and Emerging Digital Technologies and Human Rights*. HRC Res. 53/29. UN Doc. A/HRC/RES/53/29. 18 July 2023. https://docs.un.org/en/a/hrc/res/53/29.

128. UN Human Rights Council. *The Promotion, Protection and Enjoyment of Human Rights on the Internet*. HRC Res. 20/8. UN Doc. A/HRC/RES/20/8. 16 July 2012. https://digitallibrary.un.org/record/731540?ln=en&v=pdf.

129. UN Office of the High Commissioner for Human Rights. *Mapping Report: Human Rights and New and Emerging Digital Technologies*. UN Doc. A/HRC/56/45. 20 August 2024. https://www.ohchr.org/en/documents/thematic-reports/ahrc5645-mapping-report-human-rights-and-new-and-emerging-digital.

130. United Nations Office on Drugs and Crime. *Comprehensive Study on Cybercrime: Draft – February 2013*. 2013. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

131. United States Air Force. *Air Force Doctrine Publication 3-12: Cyberspace Operations*. 1 February 2023. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf.

132. United States Cyber Command. "Mission and Vision." *U.S. Cyber Command*. https://www.cybercom.mil/About/Mission-and-Vision/.

133. United States Department of Defense Office of General Counsel. "An Assessment of International Legal Issues in Information Operations." Appendix in *Computer Network Attack and International Law*, *International Law Studies*, vol. 76, edited by Michael N. Schmitt and Brian O'Donnell. US Naval War College, 2002. https://digital-commons.usnwc.edu/ils/vol76/iss1/4/.

134. United States Department of Justice. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." Press release. 19 October 2020. https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

135. Van der Vyver, Johan. "The International Criminal Court and the Concept of Mens Rea in International Criminal Law." *University of Miami International & Comparative Law Review* 12 (2004): 57–94. https://ssrn.com/abstract=1940084.

136. Wall, David. "What Are Cybercrimes?" *Criminal Justice Matters* 58, no. 1 (2004): 20.

https://www.crimeandjustice.org.uk/sites/default/files/09627250408553239.pdf .

137. Wang, Xin. "Global (Re-)Framing of Cybercrime: An Emerging Common Interest in Flux of Competing Normative Powers?" *Leiden Journal of International Law* 38, no. 2 (2025): 235. https://doi.org/10.1017/S0922156524000402.

138. Waxman, Matthew C. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." *Yale Journal of International Law* 36, no. 2 (2011): 421. https://www.jstor.org/stable/24709325.

139. Welch, Larry D. "Cyberspace – The Fifth Operational Domain." Institute for Defense Analyses, 2011. https://apps.dtic.mil/sti/pdfs/AD1124078.pdf.

140. Werle, Gerhard, and Florian Jeßberger. *Principles of International Criminal Law*. 4th ed. Oxford University Press, 2020. https://doi.org/10.1093/law/9780198826859.001.0001.

141. The White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. May 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

142. Wilmshurst, Elizabeth, Harriet Moynihan, and Tsvetelina van Benthem. *Securing Justice for Cyber-Enabled International Crimes: Legal Foundations and Practical Routes to Prosecution*. Chatham House, 2026. https://www.chathamhouse.org/sites/default/files/2026-01/2026-01-26-securing-justice-cyber-enabled-international-crimes-wilmshurst-et-al.pdf.