UCP Journal *of* Law & Legal Education
Vol. 4, Issue 1 (January – June 2026)

Protection of Critical Infrastructure Against Cyber Attacks: An International Law Perspective

Minahil Saleem*, Ghulam Rasool Kassar**, Hena Parmar**

Abstract

Critical infrastructure (CI) plays an essential role in a state's functioning. From power grids, telephone networks, medical supply centres, transit systems, and financial institutions to emergency response systems, all are essential for the effective operation of businesses and service delivery, alongside catalysing economic growth and investment. However, the advent of the internet has integrated most of the state's critical infrastructure with digital technologies, which makes it vulnerable to cyberattacks in interstate conflicts. In view of this, this research is centred on the question of the extent to which International Law accords protection to CI. The paper specifically addresses two sub-questions: (1) How are cyberattacks against CI, not resulting in direct physical destruction, regulated under international law? (2) Whether offensive cyber capabilities can be a legitimate deterrence mechanism under International Law. This research is grounded in the international legal framework governing inter-state conduct, including the principle of sovereignty, non-intervention, and prohibition of the use of force. The study uses doctrinal research methodology and relies on international treaty and customary law, decisions of the International Court of Justice, and academic writings to reach its findings. The study finds that whether a non-destructive cyberattack against CI constitutes a violation of international law or not is a question to be assessed on a case-by-case basis. The determination of the lawfulness of cyber response depends upon considerations like necessity and state attribution.

* Law Associate at M/S Riaz Ali Panhwar Law Associates and Co. Email: minahilshaikh97@gmail.com
** Advocate and Visiting Faculty Member at the Institute of Law, University of Sindh, Jamshoro, Pakistan. Email: ghulamrasoolkassar@gmail.com
*** Law Associate at M/S Riaz Ali Pahnwar Law Associates and Co. Email: henaparmar2002@gmail.com

Article History: Received: 23-05-2025; Received in revised form: 20-10-2026; Accepted: 24-10-2026.
Available online: 26-10-2026
DOI: https://doi.org/10.24312/ucp-jlle.04.01.563

CC BY OPEN ACCESS — OPEN ACCESS

Keywords: Critical Infrastructure, International Law, Cyber Attacks, Cyber Deterrence, Cyber Operations

Introduction

For years, protecting CI from physical attacks has remained a top priority for governments. Due to the significant rise in cyberattacks against CI, it is now considered more problematic for national security than physical attacks alone (Chamodya, 2024). Cyberattacks on CI can have disastrous consequences ranging from interruptions in essential services to the loss of functionality, loss of data, and manipulation in digital records (Kumar, 2024). It frequently involves transnational actors and is not limited to national borders, due to which international cooperation and harmonisation of legal standards are crucial (Kumar, 2024). According to the Global Risks Report 2026, cyber insecurity has been listed as the 6th most severe global risk (World Economic Forum, 2026). Its 2021 assessment noted that CIs are at risk of experiencing unprecedented damage from cyberattacks (World Economic Forum, 2021).

The US cyber strategy 2018 specifically mentions North Korea, China, Iran, and Russia as nations that will launch cyberattacks on the US in any crisis short of war (The White House, 2018). Later, reports of aggressive cyber operations against healthcare facilities throughout the 2020 pandemic and the 2021 ransomware attack, which severely disrupted Colonial Pipeline operations in the US (Sanger et al., 2021), have exacerbated these concerns (Milanovic and Schmitt, 2020). In May 2021, there was a ransomware attack targeting the Colonial Pipeline, which provides about half of the oil used on the East Coast (Chamodya, 2024). The attack forced the corporation to halt operations for days, which resulted in fuel shortages. To restore access to its systems, Colonial Pipeline had to pay a $4.4 million ransom (Chamodya, 2024).

Similarly, the Australian government disclosed in June 2020 that it had been the target of a cyberattack campaign that targeted its CI (Prime Minister of Australia, 2020). The Australian government subsequently adopted changes to its national security laws by passing the “National Security Law and Foreign Intervention (Amendment) Act 2018" (NSLA). Under the said legislation, any act done for a foreign entity that harms Australia's infrastructure and

threatens the nation's security constitutes a criminal offence (NSLA Act, 2018, ss 82.3, 82.4).

Likewise, in December 2015, an extremely disruptive cyberattack caused sections of Ukraine's power grid to shut down for one to six hours, depriving around 230,000 people of electricity (Zetter, 2016). It is believed that this was the first blackout induced by a cyberattack (Sanger, 2016).

In addition to these, various low-level cyber operations are being carried out by nations against CI. Information gathered from these operations may be utilised to prepare for more disruptive future operations (Symantec Critical Attack Discovery and Intelligence Team, 2017). For instance, the U.S. Department of Homeland Security & Federal Bureau of Investigation (2018) found that Russia has been attacking its critical manufacturing, energy, nuclear, commercial, water, and aviation sectors since 2016. Similarly, it was revealed in 2019 that the United States had penetrated Russia's power infrastructure not just for reconnaissance purposes but also for installing malware on systems that might be used to interfere with their functioning (Sanger & Perlroth, 2019). Nations such as the US and Russia are relying on malicious cyber operations to penetrate the CI systems of others and maintain long-term presence (Buchanan & Sulmeyer, 2016). The primary concern is that these proactive cyberattacks could be used to damage or interfere with CI's future operations. This concern became apparent during the 2022 conflict in Ukraine, which involved several cyberattacks and actions that Russia had planned to disrupt Ukraine's public services, government functions and its defensive capabilities (Microsoft, 2022). In 2024, there was an approximately 70% surge in Russian cyberattacks on Ukraine, resulting in 4,315 incidents that targeted CI, including government services, energy sectors, and defence entities. According to Ukraine's cybersecurity agency, attackers sought to disrupt operations and steal sensitive data (State Service of Special Communications and Information Protection of Ukraine, 2025).

However, according to Taiwan's National Security Bureau, Chinese cyberattacks against the island nation increased to 2.4 million attempts per day in 2024. Attackers sought to disrupt CI and steal confidential data; the number of successful attacks increased by 20% over 2023 (Analysis on China's Cyberattack Techniques in 2024).

There are no treaty provisions that directly address cyberattacks (Wrange, 2014). However, a 2013 UN report concluded that "international law, especially the Charter of the United Nations, is relevant and vital" (UNGA, 2013). The same was also highlighted in the UNGA (2015) report and further confirmed in the consensus report of 2021 (UNGA, 2021). Nevertheless, there remains ambiguity as to how the rules of international law apply.

Cyber operations against CI may or may not result in physical destruction, and they can occur outside of an armed conflict, which means that interstate warfare may not always be covered under the framework of International Humanitarian Law (IHL). Since International Law has no cyber-specific treaty, states differ on how the existing international legal framework applies to non-destructive cyber operations. The main problem is whether cyber operations against CI can hold states accountable when they do not result in physical destruction.

This paper seeks to explore the potential of international law in today's era of fifth-generation hybrid warfare. The research aims to determine how international law regulates cyber operations against CI when these operations don't cause physical damage and whether offensive cyber capabilities can be used as a legitimate and lawful means for cyber deterrence. Since the research mainly deals with peacetime cyber operations (particularly the non-destructive ones), it won't cover the difference between cyberattacks that are regulated under the IHL framework and operations that are considered the use of force. The latter part is discussed separately in the literature review. Further, to maintain brevity, the researcher uses the term "disruption" generally to cover the non-kinetic effects of cyberattacks such as loss of functionality, data destruction, data theft, suspension of critical services, etc.

The paper proceeds by first examining the existing scholarly literature on the general application of the UN Charter on cyber operations and the effects-based approach to the use of force to demonstrate the regulation of destructive cyberattacks against CI under the international legal discourse and to establish the research gap. Later, it probes into the regulation of non-destructive cyberattacks against CI. Since there is no direct connection between the non-destructive nature of a cyber operation and its legal or illegal status under international law, the decision is to be made based on legal regulation and the circumstances of each case. For that, the

researcher used Schmitt's parameters for qualitative assessment of the harm, followed by the current state practice and legal discourse on the principle of sovereignty, non-intervention and the use of force. Lastly, the researcher examines cyber deterrence and its compatibility with international law and the problem of attribution using Estonia as a case study.

Methodology

This study adopts a doctrinal research methodology to examine the research questions with an in-depth analysis of existing frameworks of international law, such as the UN Charter, Judgments of the International Court of Justice (ICJ), such as the *Corfu Channel case (1949)* and the *Nicaragua case (1986),* advisory opinions of the ICJ, the Tallinn Manual (2.0), the law of state responsibility, reports of the International Law Commission, state practices, and UN expert reports. The selected case studies of cyberattacks against Estonia in 2007, the Stuxnet Case of 2010, and Ukraine's electricity grid incidents have been used to illustrate the practical implications of cyber operations against CI and its potential role in invoking cyber deterrence.

Secondary sources include peer-reviewed academic literature, books, expert commentaries, and policy reports related to cyber incidents. At length, these sources have been examined to explore whether and to what extent International Law governs non-destructive cyberattacks against CI.

Literature Review

When we talk about the modern technological system, in particular cyber incidents, an important question arises as to whether the UN Charter applies to such incidents or not, given that such technology post-dates the Charter (Hathaway et al., 2012; Schmitt, 2017). At last, it was concurred that: "states are responsible for their use of cyber operations under their UN Charter commitments" (UNGA, 2013, 2015). Through the 2018 "Paris Call for Trust and Security in Cyberspace", many states, private organisations, and actors have agreed to be bound by international law on cyber operations. Hence, it is widely concurred that international law governs cyber operations even though there are no specific treaty provisions addressing cyberattacks (Schmitt, 2013; Wrange, 2014).

The travaux préparatoires of the UN Charter suggest that Article 2(4) establishes a presumption of illegality for "any" threat or use of force inconsistent with the purposes of the United Nations Charter (United Nations, 1945a, p. 65; United Nations, 1945b, p. 336; United Nations, 1945c, p. 387). This means that even actions not targeting a state's territorial integrity or political independence may still be in breach of prohibition. The two widely recognised exceptions are: firstly, Security Council authorisation regarding coercive and armed action under Article 41 and 42 of the UN Charter, respectively and secondly, Self-defence under Article 51 of the Charter. The ICJ, in its advisory opinion, explicitly mentions that:

"Articles 2(4) and 51 of the UN Charter apply to all uses of force, irrespective of the weapons used" (Legality of the Threat or Use of Nuclear Weapons, 1996, p. 226).

This implies that cyberattacks, when meeting certain criteria, could be considered a use of force, even if executed through information systems rather than conventional weapons. Additionally, the Tallinn Manual assumes that the UN Charter applies to cyberspace, reinforcing this interpretation (Bring, 2014, p. 13). However, the key question remained: Can a cyberattack be classified as a "use of force"?

This question is assessed through three main approaches, as given below:

(a) **The tool-based approach**: It focuses on the type and severity of cyber operations employed.
(b) **The objective-based approach**: It considers the hostile intent behind the attack.
(c) **The effects-based approach**: This approach evaluates the scale and impact of cyber operations, determining whether they reach a level comparable to conventional force.

Out of all these approaches, only the effects-based approach has received the most support (Roscini, 2014), as it allows for an impact-driven assessment of whether a cyberattack constitutes a *"force"* under international law. In contrast, the tool-based and objective-based approaches are criticised for being restrictive in their scope, which makes them incompatible with the evolving nature of cyber warfare (Roscini, 2014).

The Tallinn Manual 2.0 supported this view and defined cyberattack as: *"a cyber operation, whether offensive or defensive,*

that can reasonably cause injury or death to persons or damage or destruction of objects" (Rule 92, Tallinn Manual 2.0). It also reiterates that *"A cyber operation qualifies as a use of force as its scale and effects match a kinetic attack"* (Rule 69, Tallinn Manual 2.0).

Accordingly, the most widely accepted test for determining whether a cyber operation constitutes an illegal use of force depends on its effects. This approach is also reflected in Rule 11 of the Tallinn Manual, which states that *"a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations that rise to the level of a use of force"* (Schmitt, 2017).

Additionally, under UNGA Resolution 3314 (1974), states agreed that 'force' refers to 'armed force' as outlined in Article 2(4) of the UN Charter. Similarly, the International Group of Experts has concurred that the threshold of an armed attack is met when a certain act causes injury, death, or massive physical deterioration to property. (Schmitt, 2013, Commentary to Rule 13, para. 6). In essence, cyber operations that result in tangible physical damage in the real world may qualify as uses of force under international law. (Schmitt, 2013, Commentary to Rule 11, para. 4). For instance, Russia has conducted cyber operations linked to its war in Ukraine (Satter et al., 2022).

Hence, the most effective test for determining whether a cyberattack qualifies as a use of force is to see whether it results in physical destruction (Hathaway et al., 2012, p. 817). For example, a cyber operation that triggers an explosion or opens dam gates in a populated area would meet this threshold (Ney, 2020; Koh, 2012). In this view, cyber operations have the potential to trigger kinetic damage, either directly or indirectly. For such cases, the term "cyber kinetic attacks" has been introduced (Applegate, 2013). There is ongoing debate among experts regarding whether cyberattacks that do not result in direct death, injury, or destruction can be classified as armed attacks. The International Group of Experts did not reach a consensus on this issue (Schmitt, 2013, Commentary to Rule 11, para. 8).

Existing international legal discourse concentrates excessively on destructive cyber operations. However, there is limited consensus on how international law protects CI from non-destructive cyber operations and whether offensive cyber capabilities are a legitimate means to create cyber deterrence. The

paper addresses this gap by situating cyberattacks within a doctrinal legal framework governing inter-state conduct and analysing established parameters for the qualitative assessment of cyber operations and the minimum threshold for the violation of the principles of sovereignty, non-intervention, and the prohibition on the use of force to evaluate conditions under which a non-destructive cyberattack against CI may be prohibited under International Law.

Cyber Operations Against Critical Infrastructure Without Physical Damage

There are instances of cyber operations against CI which don't result into physical destruction. Whether such operations violate international law is required to be analysed individually for each case.

Parameters to Determine the Level of Harm

Since there is no automatic connection between the fact of lack of destruction and the legality or illegality of the operation, Professor Michael Schmitt introduced seven parameters for qualitative assessment of cyberattacks to determine the level of harm that would make it fall under the use of force (Schmitt, 2013). These factors are relevant to both cyberattacks conducted within a military conflict and those occurring independently. These include: (i) severity, (ii) immediacy, (iii) directness, (iv) invasiveness, (v) measurability of effects, (vi) military character, (vii) state involvement (Schmitt, 2013). These factors guide state evaluations of cyber operations but serve as analytical tools, not legal criteria (Schmitt, 2013, Commentary to Rule 11, para. 8).

The severity of a cyber operation is assessed based on its scope, duration, and intensity of consequences (Schmitt, 2013, pp. 45–48). A cyberattack that results in damage, devastation, or death is most likely to be classified as a use of force (Schmitt, 2013, pp. 45–48).

Cyber operations with immediate consequences are more likely to be deemed a use of force whose effects develop gradually over weeks or months. The faster the impact, the higher the likelihood of classification as a forceful act (Schmitt, 2013, pp. 45–48).

The probability of the characterisation of a cyber operation as a prohibited use of force increases with the strength of connection between its cause and effect (Schmitt, 2013, pp. 45–48).

Invasiveness measures how deeply cyber operations intrude on a state's infrastructure (Schmitt, 2013, pp. 45–48). More localised effects increase perceived invasiveness. Computer network exploitation is widely used in modern espionage and, despite being highly invasive, does not qualify as a use of force under international law, as espionage itself is not explicitly prohibited (Schmitt, 2013, Rule 66). However, actions taken to facilitate cyber espionage may still be considered a use of force in certain cases. For instance, if a military aircraft enters national airspace without consent to serve as a platform for cyber espionage, it may qualify as a use of force under international law (Schmitt, 2013, Rule 66).

Cyber operations' classification as a use of force depends on the extent to which their consequences are apparent and quantifiable. In the cyber domain, effects are often less visible compared to traditional attacks (Schmitt, 2013, pp. 45–48). However, a cyber operation with clearly measurable outcomes, such as the extent of data corruption, server disruptions, or file exfiltration, increases the likelihood of being deemed a use of force (Schmitt, 2013, pp. 45–48).

The likelihood of a cyber operation being classified as a use of force increases when it has a clear connection to military activities. A strong nexus between cyber operations and military objectives enhances the perception that the attack is forceful in nature (Schmitt, 2013, pp. 45–48).

The degree of state involvement in cyber operations significantly influences how it is perceived under international law. The closer and more direct the link between a state and the cyber operation, the higher the probability that other states will regard it as a use of force attributable to that state (Schmitt, 2013, pp. 45–48).

Non-Destructive Cyber Operations Against CI and the Application of International Law

"Cyber operation" is a broader term that means "utilisation of cyber resources to attain specific goals within or via cyberspace" (Schmitt, 2017). Cyber espionage, cyber manipulation, and

cyberattacks all come under the ambit of cyber operations (Roscini, 2014). However, it is assumed that cyberattacks are the most severe and belligerent form of cyber operations (Roscini, 2014). Others believe that damaging an operating system to the extent that one would need to reinstall it or destroying specific data may be enough to qualify as a "cyber-attack" if detrimental effects such as loss of functionality result from these actions (Gill, 2015). Situations may include instances of cyberattacks influencing election results (Willsher & Henley, 2017) or cyberattacks against power grids (Pollard, 2024), ransomware campaigns, cyber operations against healthcare facilities and research centres, etc. The paper highlights the threshold that needs to be satisfied to call a cyberattack a breach of international law, even though it does not culminate in destructive effects on CI like a kinetic attack.

Sovereignty

The principle of sovereignty is the cornerstone of the international legal framework. International Law is applicable in cyberspace, as confirmed by several declarations made by the UNGA (2015), the African Union Peace and Security Council (2024), the European Union (2017), NATO (2016), the Organisation for Security and Cooperation in Europe (2016), and individual states. However, states differ in their views on whether sovereignty constitutes an independently applicable rule whose violation renders a cyber operation unlawful (United Nations General Assembly [UNGA], 2021, pp. 12–13). The view was also shared by the specialists who created the Tallinn Manual 2.0 (Schmitt, 2017).

Regarding cyber operations, the modalities outlined in the Tallinn Manual 2.0 signify various approaches to figuring out what a "sovereignty violation" might entail:

(a) A state entity physically situated in a target nation or an individual's territory that engages in cyberattacks against them (Nicaragua vs Costa Rica, 2015).
(b) The failure of cyber infrastructure to function constitutes "damage" and thus a breach of sovereignty. The degree of functionality loss must be such that reinstalling the operating system or other software becomes necessary (Schmitt, 2017, commentary to Rule 4, para. 13).

(c) Meddling with data or services required to carry out "inherently governmental functions." (Schmitt, 2017, commentary to Rule 4, para. 15)

Several States have specifically accepted the Tallinn Manual experts' threshold for what defines a breach of sovereignty. Germany and the Netherlands expressed support for aspects of this approach (UNGA, 2021, pp. 34–35, 60–61). Canada supports territorial integrity and interference with inherently governmental functions as grounds for the violation of sovereignty (National Position of Canada, 2022). On the other hand, some states like France and Iran have proposed alternative tests to determine what constitutes a violation of sovereignty. Ministère des Armées (2019, p. 6) argues that a "mere intrusion into CI amounts to a breach of sovereignty". In a similar vein, the General Staff of the Armed Forces of the Islamic Republic of Iran (2020) has contended that "illegal access to foreign cyber infrastructure, whether public or private, may constitute a violation of sovereignty."

Prohibition of Intervention

The duty of non-intervention is codified in Article 2(7) of the UN Charter. Additionally, the UN acknowledged it as a principle of customary international law that prohibits states from direct or indirect meddling in another state's affairs, be it internal or external (UNGA, 1970). This interpretation is further supported by the ICJ ruling as follows:

"A prohibited intervention must […] be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social, and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion regarding such choices, which must remain free ones" (Nicaragua v. U.S., 1986).

A Cyber operation would be considered a prohibited intervention if it meets the following criteria:

(a) It has an impact on issues pertaining to political, economic, social, and cultural systems, as well as those involving which states have the freedom to make their own decisions (Nicaragua v. U.S., 1986, para. 205)

(b) The action must be inherently coercive in nature (Moynihan, 2020).

There are two approaches as to what amounts to coercion.

Regarding the first approach, an action is considered coercive if it could persuade the target state to take a course of action on a matter within its *domaine réservé* that it otherwise would not (Schmitt, 2017, commentary to rule 66, para. 21).

According to the second approach, an action is still coercive if it renders the targeted state incapable of governing or regulating issues within its *domaine réservé*. (Schmitt, 2017, commentary to rule 66, para. 19). This perspective varies from the last one in that it acknowledges that intervention may still occur even if the target state is not compelled to change its course of action, merely depriving it of its authority over a matter within its *domaine réservé* (Moynihan, 2020; Watts, 2015).

Intervention can take many different forms, including political and economic coercion (Pomson, 2022). A state's internal affairs revolve around issues like elections, power supply, healthcare, etc. Therefore, if there is some degree of coercion involved, the principle of non-intervention should forbid the harmful use of Information and Communication Technology (ICT) against a State (UNGA, 2021).

Sovereignty is violated whenever the non-intervention principle is broken (Mačák & Minárik, 2024). However, even if there is no coercion involved, cyber activities may nonetheless constitute a violation of sovereignty (Mačák & Minárik, 2024). Many states hold similar views regarding the applicability of the principles of sovereignty and non-intervention in both the real world and cyberspace. According to these governments, the undermentioned cyber activities ought to be prohibited by IHL:

(a) The deployment of cyber and various digital tools that compromise the accessibility, confidentiality, and reliability of critical civilian infrastructure, including satellites, underwater fibre optic cables, healthcare, transport, energy, and the financial sector, along with civilian logistical supply chains (UNGA, 2021, p. 74).

(b) Attempts to remove, destroy, or render useless objects central to the survival of masses, such as ICT infrastructure for food production or drinking water installations (UNGA, 2021, p. 74).

Prohibition of the Use of Force

As discussed in the preceding sections, Article 2(4) of the UN Charter prohibits the use of force. This prohibition is not only a component of customary international law (Occupied Palestinian Territory Advisory Opinion, 2004, para. 87; Nicaragua v. United States, 1986, para. 187-190) but is also often referred to as a peremptory norm of international law (Corten, 2021; Grey, 2018). The ICJ states that "the prohibition pertains to any use of force, irrespective of the means employed" (Legality of the Threat or Use of Nuclear Weapons, 1996). However, the definition of "force" is restricted to the use of armed force (Dörr and Randelzhofer, 2012) and to operations whose scope and outcomes are like those of using armed force (Brownlie, 1963; Schmitt, 2017, rule 69).

The question of whether cyber activities that have no tangible consequences could constitute prohibited use of force is currently a matter of debate. By 2024, state practice does not provide strong evidence to support the assertion that the definition of "force" has changed to encompass non-destructive cyberattacks directed at CI (Roscini, 2014; Tsagourias, 2012). Nevertheless, various states have started to tackle this question. Especially France, the Netherlands, and Norway allow for the possibility of cyber operations that do not result in physical harm to be considered uses of force, provided specific requirements are met (UNGA, 2021), i.e.

(a) It either directly or indirectly leads to, or has the potential to lead to, physical damage to property, fatalities, or injuries to people (Roscini, 2014; Schmitt, 2017, commentary to rule 69, para. 9a).
(b) If the disruption caused by cyber operations is "significant enough to affect state security" (Roscini, 2014).
(c) The gravity, scope, and military nature of the repercussions of a particular cyber operation (UNGA, 2021).
(d) The conditions that existed at the time of the operation, including how it began and the type of instigator (military or otherwise) (Ministère des Armées, 2019).

Given the foregoing thresholds, the 2010 Stuxnet attack that was thought to have been intended to destroy Iran's nuclear infrastructure, probably to thwart the country's uranium enrichment program (Hafezi, 2010) and which was seen to be the first ever cyber-attack that caused destructive effects (Walsh, 2010) would

fall under the prohibition of "use of force" as the ensuing interruption was sufficient to effect the security of state, a threshold highlighted by Roscini (2014) and Schmitt (2017). Additionally, the 2015 power grid cyberattack in Ukraine, which occurred during the ongoing Russo-Ukrainian War (2014–present) and caused power outages for almost 225,000 consumers in Western Ukraine, disabling or destroying IT infrastructure components (Polityuk, 2016), destruction of files stored on servers was arguably an attack likely to result in direct or indirect physical harm to property, death, or injury to people, and substantial enough to affect state security, thereby qualifying as the use of force.

Many of the criteria are also captured in the Tallinn Manual (Schmitt, 2013, 2017). Additionally, a variety of states agreed in the official UN report that actions that disrupted essential services without inflicting physical damage were covered under the use of force prohibition (UNGA, 2021). Further, a cyber action that significantly hampers state functions, such as by deploying crypto viruses or causing digital sabotage against public or private power grids, telecommunications systems, financial institutions, or sabotaging the supply of COVID-19 vaccines, might be seen as a violation of Article 2(4) (UNGA, 2021).

An operation may violate other elements of international law even if it falls short of the threshold for the use of force (Egan, 2016; Wright, 2018). This includes transgressions of the principles of sovereignty and non-intervention. The target-based or strict liability approach supports this position by stating that:

'By their very nature, it should be assumed that a state has hostile intent when it infiltrates sensitive computer systems, such as missile defence computer systems, early warning or command and control systems, and other computers that ensure the security and dependability of a nuclear stockpile.' (Sharp, 1999). This principle states that the right to self-defence can be invoked by a state in response to any attack targeting its CI.

The Potential and Applicability of Cyber Deterrence and Offensive Cyber Capabilities

Cyber deterrence is a means to restrain opponents from attacking a nation's physical and digital infrastructure (Knapp & Boulton, 2006). Protecting CI requires robust and effective

deterrence capabilities. In essence, cyber deterrence involves two approaches:

Cyber Deterrence by Denial

Deterrence by denial methods reduce the potential benefits of cyberattacks by taking targets offline, making them impenetrable, or making attacks ineffective. Such a form of deterrence can enhance resilience, enable recovery, and can also diminish the motivation for some assaults by rendering them fruitless. Since cyber deterrence is effective when the decision is based on cost-benefit comparison, deterrence by denial methods undermine this cost-benefit framework by depleting the assailant's time and assets (Nye, 2017). Further, since attackers possess constrained resources and time, increasing costs can dissuade assaults. Bruce Schneier emphasises that the fundamental strategies for augmenting effort, elevating risk, and diminishing rewards apply equally to cybersecurity and crime prevention: fortifying targets; regulating access to premises; monitoring exits; identifying offenders; managing tools; enhancing surveillance; employing place managers; mitigating peer pressures; among others (Schneier, 2012). One notable example of denial-based deterrence is Israel's "Iron Dome", an AI-driven defence system, interested in the protection of CI from opponents' cyber threats (Raska, 2014).

Cyber Deterrence by Punishment

Deterrence by punishment, in the context of cyberattacks, is an offensive cyber capability to create cyber deterrence. The objective of deterrence through punishment is to avert aggression by threatening more severe aggression, manifested as painful and potentially lethal retaliation. Concrete retaliation against an adversary's cyberattacks is part of deterrence by punishment, which may cause more harm than first thought. The anonymity maintained by attackers and the attribution dilemma, however, provide unique challenges in the online realm and frequently make it more difficult to quickly identify and punish the guilty individual (Nye, 2017). One such example is the Stuxnet case, in which attribution and the ensuing punishment were extremely difficult due to the attack's clandestine nature (Shackelford & Andres, 2010).

Although deterrence by denial methods reduce the potential benefits of cyberattacks, they alone do not stop cyberattacks. To make deterrence work, adversaries must incur punishments. Without effective deterrence, enemies will keep trying unsuccessful cyberattacks until they find a solution (Goodman, 2010). For cyber retaliation to be effective, the deterrent state must first identify the target of the counteraction, which is more complex due to attribution issues in cyberattacks. In the cyber domain, cyber deterrence closely parallels conventional deterrence (Goodman, 2010). A victimised state must evaluate the consequences before revenge; if it cannot equate with its opponent in an expanding sequence of reprisals, it should abstain from retaliation altogether (Long, 2017).

Integration of Cyber Deterrence with International Law

According to international law, while utilising the option of cyber deterrence, states must give due consideration to the principles of proportionality and necessity and the principle of use of force prohibition (Schmitt, 2017). This legal clarity aims to protect the deterring state's vital infrastructure from further retaliation, which will guarantee that the cyber deterrence in response to a cyberattack that amounts to the use of force falls under its exception, enshrined under Article 51 of the Charter (Schmitt, 2017).

Cyber Deterrence and the Challenge of Attribution

A primary reason some experts question the effectiveness of deterrence in cyberspace is the difficulty of reliably attributing cyberattacks to their actual perpetrators (Nye, 2017). In 2010, US Deputy Secretary of Defence William Lynn stated, "A computer virus usually doesn't have a return address, but a missile does." If identification is possible at all, the forensic analysis needed to find a criminal could take months (Lynn, 2010). Identifying a machine's true location is different from identifying an attack's perpetrator. Initial perceptions may be wrong (Chon, 2015). The 2012 JPMorgan Chase bank attack that stole seventy-six million records was blamed on Russia. However, in 2015, the U.S. Justice Department discovered a professional criminal gang in Tel Aviv and Moscow that was headed by two Israelis and a U.S. citizen (Nakashima,

2015). In this case, it can be assumed that fast attribution deters, as effective forensic and intelligence gathering takes time and may even take years (Clark & Landau, 2010).

Thus, timely attribution is frequently challenging and expensive, but feasible. Rid and Buchanan (2015) assert that a government's technical expertise enhances its capacity to conceal its secret activities, detect those of others, and respond appropriately. Currently, Governments are enhancing their capacities, while numerous non-state private-sector organisations are also establishing a market for attribution, hence decreasing the financial burden on governments to reveal sensitive sources. While the issue of attribution cannot be underestimated, flawed attribution does not exclude a certain level of cyber deterrence through deterrence by punishment (Clark & Landau, 2010). The cases of Estonia and Georgia cyber warfare demonstrate that attribution is not the formidable obstacle that theoretical models imply because of interdependence and counterproductivity that are significant in the cyber world (Goodman, 2010).

Case Study: Estonia (2007)

A significant cyberattack occurred in Estonia in 2007 (Ottis, 2008). Numerous denial-of-service attacks that targeted state-run internet sites, digital banking, mainstream media, and other information channels temporarily stopped the regular functioning of the country's digital infrastructure. For Estonia, it served as a warning that led to extensive investments in cyber resilience for the protection of its CI. Since then, international cyberattacks like NotPetya, WannaCry, and SolarWinds have not seriously harmed Estonia, demonstrating the success of the nation's deterrence tactics (Pernik, 2021).

To foster responsible governmental conduct in cyberspace, the first element of Estonia’s cyber deterrence depends on initiatives to strengthen entanglement and mould cyber rules and regulations. To do this, the Estonian government founded the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn in partnership with the North Atlantic Treaty Organisation (NATO) (Robinson & Hardy, 2021). As a result, Estonia has a significant leadership position and a stake in determining how legal principles like sovereignty ought to be applied in cyberspace (Budnitsky, 2022).

Further, the third edition of the Tallinn Manual has been developed by the CCDCOE to date (Clark, 2024). In the event of another significant cyberattack, Estonia can utilise Article 5 of NATO since it defines a cyberattack as a use of force and a violation of sovereignty. Non-NATO members have ceased launching strategic cyberattacks against Estonia because of this strong deterrent effect.

The secondary element of Estonia's cyber deterrence is denial, restricting the prospects of penetration of cyberattacks into its CI. The government has focused its investments since 2008 on strengthening important infrastructure, networks, and assets (Jayakumar, 2020). Estonia employed technologies like multi-factor authentication and cloud storage to protect its CI operations from cyberattacks (Jayakumar, 2020). These efforts proved instrumental in reducing present cyber threats in Estonia even though they were not specifically intended to create cyber deterrence (Jayakumar, 2020). These activities simultaneously preclude advantages for aggressors and enhance cyber deterrence. On the same lines, Estonia actively mobilises its civilian population as part of its strategy for cyber deterrence by denial (Stoakes, 2024). To do so, the Estonian Defence League's Cyber Unit was founded in the wake of the 2007 incident. The unit trains them to become experts in cybersecurity (Kaska et al., 2013).

Estonia employs the third tier of cyber deterrence, which is punishment through name-shaming (Oh, 2019). Since enacting a public attribution policy in 2019, the Estonian government has regularly employed public attribution as a form of punishment to harm an adversary's reputation (Vostoupal & Uhlířová, 2024). For instance, the Estonian government recently attributed the October 2019 cyberattacks against Georgia to Russia, stating: “We are certain that Russia's military intelligence agency (the GRU) carried out these cyberattacks in an effort to sow discord and disrupt the lives of common Georgians.” (Statement of Foreign Minister of Estonia, 2020).

Because of the above-mentioned problems with attribution, some have argued that public attribution is a poor method of punishment-based deterrence (De Spiegeleire, 2020). Since 2020, the Estonian government has been the victim of many significant cyberattacks that have not yet been linked (Pernik, 2021). However, experts contend that public attribution is more crucial for promoting responsibility in cyberspace in compliance with international rules

and standards. It is also important to keep in mind that the measures taken by Estonia to hold adversaries liable for cyberattacks were partly supported by its EU and NATO allies. Estonia, on its own, has limited options for taking punitive action against a hostile state, just like any other state. Therefore, Estonia's experience with cyber deterrence demonstrates that states can effectively adopt a defence-dominant posture.

Conclusion

Concisely, international law applies to cyber operations even though no cyber-specific treaty exists. The 2015 UN GGE report affirmed that the Charter applies to intentional damage to CI inflicted by cyber operations. The Tallinn Manual 2.0 extended this analysis to non-kinetic cyber operations, covering sovereignty, non-intervention and due diligence (Schmitt, 2017). Whether a non-destructive cyberattack against CI constitutes a violation of international law or not is an open question to be assessed case by case depending on the severity, (ii) immediacy, (iii) directness, (iv) invasiveness, (v) measurability of effects, (vi) military character, and (vii) state involvement. The research further establishes that the principle of sovereignty and non-intervention applies to non-destructive cyberattacks once the relevant thresholds are met. A cyberattack against CI amounts to prohibited intervention only where it is coercive (such as ransomware attacks) and affects a matter that lies inherently within a state's domestic jurisdiction (like elections and power distribution, etc.). However, sovereignty remains contested as a standalone rule against cyberattacks. But the majority view, i.e., France, Germany, Netherland and others endorse it as such. Lastly, this research establishes that an offensive cyber response is not automatically lawful. That's because the Tallinn experts treat necessity as binding. If cyber-operations below the use of force level suffice to deter or repel an armed attack, forceful responses are barred (Schmitt, 2017). Also, attribution is a precondition because wrongly attributed responses amount to their own wrongful acts and risk escalation. Estonia's case study is consistent with these elements. Since the attribution remained unsettled and the effects of the cyberattack remained below the use-of-force criteria, the formation of a cyber defence unit and its non-offensive advisory role demonstrates that a defence-dominant

posture is both practicable and consistent with the legal limits discussed above.

References

African Union Peace and Security Council. (2024, January 29). Common African position on the application of international law to the use of information and communication technologies in cyberspace. https://papsrepository.africa-union.org/bitstream/handle/123456789/2022/1196%20AU%20Common%20Position%20Adopted%20Version%20-%20EN.pdf?sequence=11&isAllowed=y

Analysis on China's Cyberattack Techniques in 2024. Retrieved from https://www.nsb.gov.tw/en/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/7d118bec-6a18-4e95-ad85-4055fc48cc31.pdf.

Applegate, S. D. (2013). The dawn of kinetic cyber. In K. Podins, J. Stinissen, & M. Maybaum (Eds.), Proceedings of the 5th International Conference on Cyber Conflict (pp. 1–14). NATO Cooperative Cyber Defence Centre of Excellence. Available at https://ccdcoe.org/uploads/2018/10/10_d2r1s4_applegate.pdf

Bring, O. (2014). The use of force under the UN Charter: Modification and reform through practice or consensus. In J. Ebbesson, M. Jacobsson, M. Klamberg, D. Langlet, & P. Wrange (Eds.), International law and changing perceptions of security: Liber Amicorum Said Mahmoudi (pp. 1–13). Brill | Nijhoff. https://doi.org/10.1163/9789004274587_002

Brownlie, I. (1963). International law and the use of force by states. Oxford University Press.

Buchanan, B., & Sulmeyer, M. (2016). Russia and cyber operations: Challenges and opportunities for the next U.S. administration. Carnegie Endowment for International Peace. https://carnegieendowment.org/posts/2016/12/russia-and-cyber-operations-challenges-and-opportunities-for-the-next-us-administration

Budnitsky, S. (2022). A relational approach to digital sovereignty: E-Estonia between Russia and the West. International Journal of Communication, 16, 22-22.

Chamodya, N. (2024). Critical infrastructure and the importance of safeguarding it in the Digital age, Medium. Available at: https://blog.bugzero.io/critical-infrastructure-and-the-importance-of-safeguarding-it-in-the-digital-age-10ddfd3ba188 (Accessed: 03 March 2025).

Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS 16 (UN Charter) art. 2(4).

Chon, G., Kuchler, H., & Scannell, K. (2015). FBI Probes Possible China Military Involvement in Cyber Attack. Financial Times.

Clark, D. D., & Landau, S. (2010). Untangling attribution. In Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. policy (pp. 25–40). National Research Council.

Clark, I. A. (2024). International Research Cooperation in The Tallin Manual. Granite Journal: The University of Aberdeen Postgraduate Interdisciplinary Journal, 9(1), 2.

Corten, O. (2021). The law against war: The prohibition on the use of force in contemporary international law (2nd ed.). Hart Publishing. https://doi.org/10.5040/9781509949021

De Spiegeleire, S., Holynska, K., Batoh, Y., & Sweijs, T. (2020). Reimagining Deterrence: Towards Strategic (Dis) Suasion Design. Hague Centre for Strategic Studies.

Dörr, O., & Randelzhofer, A. (2012). Article 2 (4). In B. Simma, D.-E. Khan, G. Nolte, A. Paulus, & N. Wessendorf (Eds.), The Charter of the United Nations: A commentary (3rd ed., Vol. 1, pp. 200–234). Oxford University Press. https://doi.org/10.1093/law/9780199639762.003.0010

Egan, B. J. (2016, November 10). Remarks on international law and stability in cyberspace. U.S. Department of State. https://2009-2017.state.gov/s/l/releases/remarks/264303.htm

European Union. (2017, November 20). Council conclusions on the Joint Communication to the European Parliament and the Council: Resilience, deterrence and defence: Building strong cybersecurity for the EU.

https://www.consilium.europa.eu/media/31666/st14435en17.pdf

General Staff of the Armed Forces of the Islamic Republic of Iran. (2020, July). Declaration of the General Staff of the Armed Forces of the Islamic Republic of Iran regarding international law applicable to the cyberspace. NourNews. https://nournews.ir/en/news/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat

Gill, T. D. (2015). International humanitarian law applied to cyber-warfare: Precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict. In N. Tsagourias & R. Buchan (Eds.), Research handbook on international law and cyberspace (pp. 366–379). Edward Elgar Publishing. https://doi.org/10.4337/9781782547396.00029.

Goodman, W. (2010). Cyber deterrence: Tougher in theory than in practice? Strategic Studies Quarterly, 4(3), 102-135.

Grey, C. (2018). International Law and the use of force. Oxford University Press, p. 32.

Hafezi, P. (2010, November 29). Iran admits cyber attack on nuclear plants. Reuters. https://www.reuters.com/article/us-iran-idUSTRE6AS4MU20101129

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attacks. California Law Review, 100(4), 817–886. https://doi.org/10.15779/Z38DF6V ;

International Court of Justice. (1949). Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania): Judgment of 9 April 1949 (Merits). I.C.J. Reports 1949, 4.

International Court of Justice. (1986). Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, Judgment. I.C.J. Reports 1986, p. 14. Retrieved from https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

International Court of Justice. (2015). Certain activities carried out by Nicaragua in the border area (Costa Rica v. Nicaragua); Construction of a road in Costa Rica along the San Juan

River (Nicaragua v. Costa Rica), judgment, I.C.J. Reports 2015, p. 665.

Jayakumar, S. (2020). Cyber-attacks by terrorists and other malevolent actors: Prevention and preparedness with three case studies on Estonia, Singapore, and the United States. Handbook of terrorism prevention and preparedness, 871-925.

Kaska, K., Osula, A.-M., & Stinissen, J. (2013). The cyber defence unit of the Estonian Defence League: Legal, policy and organisational analysis. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/library/publications/the-cyber-defence-unit-of-the-estonian-defence-league-legal-policy-and-organisational-analysis/.

Knapp, K. J., & Boulton, W. R. (2006). Cyber-warfare threatens corporations: Expansion into commercial environments. Information Systems Management, 23(2), 76–87. https://doi.org/10.1201/1078.10580530/45925.23.2.20060301/92675.8.

Koh, H. H. (2012, September 18). International law in cyberspace. U.S. Department of State. https://2009-2017.state.gov/s/l/releases/remarks/197924.htm

Kumar, A. (2024, December). Examining cybersecurity laws: Protecting critical infrastructure against emerging threats and global cybercrime. Journal of Law and Intellectual Property Rights, 1(1), 21–29.

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004, p. 136. https://www.icj-cij.org/files/case-related/131/131-20040709-ADV-01-00-EN.pdf

Legality of the threat or use of nuclear weapons (Advisory Opinion), I.C.J. Reports 1996, 226. https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

Long, A. (2017). A cyber SIOP? Operational considerations for strategic offensive cyber planning. Journal of Cybersecurity, 3(1), 19-28.

Lynn, W. J., III. (2010). Defending a new domain: The Pentagon's cyberstrategy. Foreign Affairs, 89(5), 97–108.

https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Mačák, K., & Minárik, T. (2024, September 24). Scenario 01: Election interference. In International cyber law: Interactive toolkit. NATO Cooperative Cyber Defence Centre of Excellence. https://cyberlaw.ccdcoe.org/wiki/Scenario_01:_Election_interference

Microsoft. (2022, April 27). Special report: Ukraine—An overview of Russia's cyberattack activity in Ukraine. https://www.microsoft.com/en-gb/security/security-insider/intelligence-reports/special-report-ukraine/

Milanovic, M., & Schmitt, M. N. (2020). Cyber attacks and cyber (mis)information operations during a pandemic. Journal of National Security Law & Policy, 11(1), 247–284. https://jnslp.com/2020/10/19/cyber-attacks-and-cyber-misinformation-operations-during-a-pandemic/

Ministère des Armées. (2019). International law applied to operations in cyberspace. https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf

Ministry of Foreign Affairs of the Republic of Estonia, "Statement of the Foreign Minister of the Republic of Estonia Urmas Reinsalu," 20 February 2020, https://vm.ee/en/news/statement-foreign-minister-republic-estonia-urmas-reinsalu?utm_source=chatgpt.com.

Moynihan, (2020), 'The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace' 6(3) Journal of Cyber Policy 394, 400-1.

Nakashima, E. (2015, July 21). U.S., Israel make arrests in schemes thought to be tied to JPMorgan hack. The Washington Post. https://www.washingtonpost.com/world/national-security/us-israel-make-arrests-in-schemes-thought-to-be-tied-to-jpmorgan-hack/2015/07/21/321ebcaa-2fd7-11e5-97ae-30a30cca95d7_story.html?utm_source=chatgpt.com.

National position of Canada (2022). In International cyber law: Interactive toolkit. NATO Cooperative Cyber Defence Centre of Excellence. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Canada_(2022)#Prohibition_of_intervention

National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 (Cth) sch 1 pt 1 div 82; Revised Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth) 62 [137]

Ney, P. C., Jr. (2020, March 2). Remarks at U.S. Cyber Command legal conference. U.S. Department of Defense. https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

North Atlantic Treaty Organization. (2016, July 9). Wales Summit Declaration. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

Nye, J. S., Jr. (2017). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266.

Oh, L. "Exploring Policy Conditions for Cyber Deterrence: A Case Study of Estonia," Cornell International Affairs Review 12, no. 2 (2019): 121–158, https://ecommons.cornell.edu/entities/publication/538154c1-5faf-4cb6-9a79-6883ecbf7acb.

Organization for Security and Co-operation in Europe. (2016, March 10). Decision No. 1202: OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies (PC.DEC/1202). https://www.osce.org/pc/227281

Ottis, R. (2008, July). Analysis of the 2007 cyber-attacks against Estonia from the information warfare perspective. In Proceedings of the 7th European Conference on Information Warfare (p. 163). Reading, MA: Academic Publishing Limited.

Pernik, P. (2021). Cyber deterrence: A case study on Estonia's policies and practice (Hybrid CoE Paper 8). European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-paper-8-cyber-deterrence-a-case-study-on-estonias-policies-and-practice/?utm_source=chatgpt.com.

Polityuk, P. (2016, January 27). Hackers have infiltrated Ukraine's power grid—and they could take down other infrastructure

at any time. Business Insider. https://www.businessinsider.com/r-exclusive-hackers-may-have-wider-access-to-ukrainian-industrial-facilities-2016-1

Pollard, M. (2024). A case study of Russian cyber-attacks on the Ukrainian power grid: Implications and best practices for the United States. Pepperdine Policy Review, 16(1), Article 1. https://digitalcommons.pepperdine.edu/ppr/vol16/iss1/1/.

Pomson, O. (2022). The prohibition on intervention under international law and cyber operations. International Law Studies, 99, 180–219. https://digital-commons.usnwc.edu/ils/vol99/iss1/7/

Prime Minister of Australia. (2020, June 19). Statement on malicious cyber activity against Australian networks. https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks

Raska, M. (2014, October 2). Building a cyber–Iron Dome: Israel's cyber defensive envelope. S. Rajaratnam School of International Studies. https://rsis.edu.sg/rsis-publication/rsis/co14192-building-a-cyber-iron-dome-israels-cyber-defensive-envelope/

Rid, T., & Buchanan, B. (2015). Attributing cyber-attacks. Journal of Strategic Studies, 38(1-2), 4-37.

Robinson, N., & Hardy, A. (2021). Estonia: From the "Bronze Night" to cybersecurity pioneers. In Routledge Companion to Global Cyber-Security Strategy (pp. 211-225). Routledge.

Roscini, M. (2014), "Cyber Operations and the Use of Force in International Law". Oxford University Press. 59.

Sanger, D. E. (2016, February 29). Utilities cautioned about potential for a cyberattack after Ukraine's. The New York Times. https://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html

Sanger, D. E., Krauss, C., & Perlroth, N. (2021, May 8). Cyberattack forces a shutdown of a top U.S. pipeline. The New York Times. https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

Sanger, D. E., & Perlroth, N. (2019, June 15). U.S. escalates online attacks on Russia's power grid. The New York Times.

https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

Satter, R., Bing, C., & Stubbs, J. (2022, January 24). Ukraine's computers hit by data-wiping software as Russia launched invasion. Reuters. https://www.reuters.com/

Schmitt, M. N. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on International Law Applicable to Cyber Operations (Rule 11). Cambridge University Press.

Schneier, B. (2012). Liars and outliers: enabling the trust that society needs to thrive. John Wiley & Sons.

Shackelford, S. J., & Andres, R. B. (2010). State responsibility for cyber-attacks: competing standards for a growing problem. Geo. J. Int'l L., 42, 971.

Sharp, W. G. (1999), "CyberSpace and the Use of Force". Aegis Research Corporation, p. 130.

Stoakes, E. (2024). Toward a self-defence model for media in small democracies: responding to weaponised information in the 'new cold war' environment.

Symantec Critical Attack Discovery and Intelligence Team. (2017, October 20). Dragonfly: Western energy sector targeted by sophisticated attack group. Symantec Threat Intelligence. https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. Journal of Conflict and Security Law, 17(2), 229–244. https://doi.org/10.1093/jcsl/krs019

United Nations. (1945a). Documents of the United Nations Conference on International Organisation, San Francisco, 1945 (Vol. 6, Document 1123, I/8, p. 65).

United Nations Information Organisations; United Nations. (1945b). Documents of the United Nations Conference on International Organisation, San Francisco, 1945 (Vol. 6, Document 784, I/1/27, p. 336).

United Nations Information Organisations; United Nations. (1945c). Documents of the United Nations Conference on International Organisation, San Francisco, 1945 (Vol. 6, Document 885, I/1/34, p. 387).

United Nations General Assembly. (1970, October 24). Declaration on principles of international law concerning friendly relations and cooperation among states in accordance with the Charter of the United Nations (Resolution 2625 (XXV)). https://docs.un.org/en/A/RES/2625(XXV)

United Nations General Assembly. (1974). Definition of aggression (A/RES/3314(XXIX)). https://digitallibrary.un.org/record/190983.

United Nations General Assembly. (2013, June 24). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98). https://docs.un.org/en/A/68/98

United Nations General Assembly. (2015, July 22). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174). https://digitallibrary.un.org/record/799853

United Nations General Assembly. (2021, March 10). Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final substantive report (A/AC.290/2021/CRP.2). https://digitallibrary.un.org/

United Nations General Assembly. (2021, July 13). Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States (A/76/136). https://digitallibrary.un.org/record/3933543/files/A_76_136-EN.pdf

United Nations Information Organisation. (1945a). Documents of the United Nations Conference on International Organisation, San Francisco, 1945: Vol. III. Dumbarton Oaks proposals, comments and proposed amendments.

United Nations Information Organisation. (1945b). Documents of the United Nations Conference on International Organisation, San Francisco, 1945: Vol. VI. Commission I: General provisions.

U.S. Department of Homeland Security, & Federal Bureau of Investigation. (2018, March 15). Russian government cyber

activity targeting energy and other critical infrastructure sectors (Technical Alert TA18-074A). https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical-infrastructure-sectors

Vostoupal, J., & Uhlířová, K. (2024). Of hackers and privateers: The possible evolution of the problem of cyber-attribution. Masaryk University Journal of Law and Technology, 18(2), 169-214.

Vulnerability Detection and Cyber Incident/Cyber Attack Response System. State Service of Special Communications and Information of Protection of Ukraine. 2025. Retrieved from https://scpc.gov.ua/api/files/87f65677-dc26-40d1-85c5-f6e3ce31f158.

Walsh, C. (2010, October 7). US prepares for cyber threats in the wake of suspected "Stuxnet" attack in Iran. Harvard National Security Journal. http://harvardnsj.org/2010/10/us-prepares-for-cyber-threats-in-the-wake-of-suspected-stuxnet-attack-in-iran/

Watts, S. (2015). Low-intensity cyber operations and the principle of non-intervention. In J. D. Ohlin, K. Govern, & C. Finkelstein (Eds.), Cyber war: Law and ethics for virtual conflicts (pp. 249–270). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198717492.003.0012

The White House. (2018, September). National cyber strategy of the United States of America. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Willsher, K., & Henley, J. (2017, May 6). Emmanuel Macron's campaign hacked on eve of French election. The Guardian. https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election

World Economic Forum (2021) The Global Risks Report 2021. 16th Edition, World Economic Forum, http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

World Economic Forum. (2026, January 14). The global risks report 2026. https://www.weforum.org/publications/global-risks-report-2026

Wrange, P. (2014). Intervention in national and private cyberspace and international law. In J. Ebbesson, M. Jacobsson, M. Klamberg, D. Langlet, & P. Wrange (Eds.), International law and changing perceptions of security: Liber Amicorum Said Mahmoudi (pp. 307–326). Brill | Nijhoff. https://doi.org/10.1163/9789004274587_019

Wright, J. (2018, May 23). Cyber and international law in the 21st century. Attorney General's Office, GOV.UK. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. WIRED. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/