ACTA SCIENTIAE

ISSN: 2178-7727

International Law in Cyberspace: Challenges of Sovereignty, Attribution, Enforcement and Global Cyber Governance

Hitika Singh[1], Asha Verma[2], Myunghoon Roh[3]

[1]School of Law, Manav Rachna University, Faridabad, Haryana, India, singhhitika72@gmail.com
[2]School of Law, Manav Rachna University, Faridabad, Haryana, India, asha19april@gmail.com
[3]Department of Criminal Justice and Criminology, Salve Regina University, Newport, Rhode Island, United States, myunghoon.roh@salve.edu

ABSTRACT

The fast pace of development of digital technologies has turned cyberspace into an important sphere of international relations and created numerous legal problems in the context of the application of international law to cyberspace. To begin with, cyber operations transcend borders and involve not only government entities but also non-state actors as well, breaching the rules of conduct for states. The current research paper will deal with the applicability of international law to cyberspace from the perspective of sovereignty, non-intervention, prohibition of the use of force, attribution, state responsibility, and enforcement. The research methodology of this work is going to be the doctrine of legal research. It will analyze such international instruments as the United Nations Charter, customary international law, the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), the Tallinn Manual 2.0, and others. The paper argues that for the development of an effective and sustainable framework of global cyber governance, it is crucial to foster international collaboration, clarify the implementation of current legal principles, and enhance consistency among states in their actions.

KEYWORDS: International Law, Cyberspace, Cyber Governance, Sovereignty, Attribution, State Responsibility, Cybersecurity.

INTRODUCTION

Cyberspace has been recognized as an important realm in international relations, providing means for the administration of governments, military activities, international trade, financial dealings, and communication across borders (Schmitt, 2021). Digitalization in societies has essentially changed the way states govern their citizens, deal with other states, and provide basic public services (Tsagourias & Buchan, 2021). With the integration of digital technologies in state governance and development, there has also been increased vulnerability of states to cyber threats aimed at governmental agencies, financial systems, health care delivery, energy sector, and telecom companies (Healey, 2013; Shackelford, 2014)). As a result, cybersecurity has evolved from a primarily technological sector to one that is extremely important for global governance, peace, and security (Tsagourias & Buchan, 2021). Given these developments, the UN Group of Governmental Experts (UNGGE) recognized that the use of ICT is important for global security and that governments' actions in cyberspace are nonetheless subject to international law (United Nations, 2015). Cyber operations have become an integral part of the modern-day security environment due to their increased complexity and number. The nature of cyberattacks is no longer limited to stealing information or disrupting networks, but these attacks have become such strategies that may affect diplomatic relations, military affairs, elections, and economic stability (Nye, 2017). Some examples of such attacks are cyberattacks on Estonia in 2007, the Stuxnet attack aimed at Iran's nuclear program, the WannaCry ransomware attack, and SolarWinds supply chain attack.

All the mentioned attacks prove the ability of cyber operations to create far-reaching political, economic, and security impacts without using any conventional weapons (Healey, 2013; Rid & Buchanan, 2015). Such developments have become a challenge to the traditional understanding of conflict due to the blurring of boundaries between peace and war and the inefficiency of the existing legislation developed to regulate geographical warfare. While land, maritime, air, and space have traditionally been recognized as separate fields for operations, the cyberspace domain is known for its absence of territorial limitations to the system

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

architecture, its decentralized infrastructure, and the prevalence of privately owned digital infrastructure (Schmitt, 2021). Cyber operations usually take place within seconds across several jurisdictions, hide the identity of the attacker through anonymization measures, and often involve non-state actors that operate outside state territories (Hathaway et al., 2012). These particular features create difficulties when applying fundamental rules of international law established within a jurisdictional framework (Schmitt, 2017). The issues related to jurisdiction, sovereignty, due diligence, attribution, and accountability thus become more complex in cyberspace than in traditional international disputes (Tsagourias, 2015).

Even with all of these innovations, it has been agreed by the international community at large that cyberspace is no legal vacuum. Article 2(4) of the Charter of the United Nations still bars the threat or use of force in international relations (United Nations, 1945), while customary international law, law of state responsibility, and general principles of international law are applicable to cyber operations (Schmitt, 2017). It has been reiterated by UNGGE that the Charter of the United Nations is applicable to the use of ICTs by states (United Nations, 2013, 2015, 2021). Likewise, the OEWG has stressed on the significance of responsible state behaviour, confidence-building measures, capacity building, and international cooperation for peace and stability in cyberspace (United Nations, 2021). However, despite the acceptance of the applicability of international law, no consensus has been reached about its interpretation and implementation (Efrony & Shany, 2018). The topic of cyber sovereignty is one of the most contentious. States continue to disagree on whether certain cyber activities can be deemed a violation of territorial sovereignty on their own or only result in other violations of existing obligations under international law, despite the fact that sovereignty has long been one of the pillars of international law. While the UK was less inclined to apply sovereignty as an autonomous norm, France and the Netherlands have interpreted the concept of cyber sovereignty rather broadly (Efrony & Shany, 2018). Despite being essential to international legal order, it becomes obvious that the legal status of sovereignty in cyberspace is ambiguous (Tsagourias & Buchan, 2021).

No less controversial has been the implementation of the rules concerning non-intervention and the prohibition on the use of force. While international law does not permit coercive action in matters that belong to the internal affairs of another country, establishing whether a cyber operation amounts to unlawful intervention raises difficult questions of law (Roscini, 2014). So too has there been legal controversy surrounding the interpretation of Article 2(4) and Article 51 of the UN Charter in relation to the situations in which cyber operations could constitute a prohibited use of force or an armed attack entitling self-defense (Dinstein, 2021). In an effort to address these emerging issues, there have been many international efforts designed to define the application of international law in relation to cyberspace. One of the major attempts in this regard is the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, which stands out as one of the most extensive analyses of how international law can be applied to cyberspace (Schmitt, 2017). Despite the fact that the Manual does not create any legal obligations, it has made a considerable contribution to the academic discourse, development of the state legal positions and further elaboration of the international norms related to cyber issues. The same applies to the Budapest Convention on Cybercrime, which serves to facilitate international cooperation in addressing transnational cybercrime (Council of Europe, 2001).

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

Hanoi Convention		Budapest Convention
Adopted by UN General Assembly in 2024 following a five-year negotiation process proposed by Russia. UN-led consensus initiative	**Adoption and Origin**	**Opened for signature in 2001 as a Council of Europe initiative involving Western observer states.** Council of Europe framework
Requires 40 ratifications to enter into force; currently holds 3 ratifications and 74–76 signatories. Emerging global instrument	**Ratification and Participation**	**Entered into force in 2004; currently maintains 81 states party including major non-European nations.** Established international standard
The United States and India have declined to sign the agreement. Excludes key Western powers	**Notable Non-Participants**	**Russia is not a party, having historically rejected the treaty as being too European-centric.** Excludes Russian participation
Faced opposition from groups like Human Rights Watch and EFF regarding vague definitions and human rights risks. Concerns over authoritarian misuse	**Civil Society Criticism**	**Criticized historically for its Western-centric drafting process and lack of global inclusivity.** Concerns over regional bias

Table 1: Comparative Global Cybercrime Treaty Architecture — UN Convention against Cybercrime vs. Budapest Convention

(**Source:** United Nations Office on Drugs and Crime. (2024). United Nations Convention against Cybercrime (UN General Assembly Resolution 79/243); Council of Europe. (n.d.). Chart of Signatures and Ratifications of Treaty No. 185: Convention on Cybercrime (Budapest Convention))

In light of this, this study evaluates international law's efficacy in regulating cyberspace. The influence of international collaboration on handling contemporary cyber threats will be taken into consideration while evaluating the legal principles of sovereignty, non-intervention, prohibition on the use of force, attribution, state accountability, and enforcement. This study will argue that although the current body of international law provides a solid normative foundation for regulating state behavior in cyberspace, it still faces significant obstacles in the form of ongoing interpretation disputes, attribution problems, jurisdictional limitations, and a lack of efficient enforcement tools, all of which impede the development of an efficient and cohesive framework of international cyber governance.

THE APPLICABILITY OF INTERNATIONAL LAW TO CYBERSPACE

2.1 The Development of Cyberspace as a Legal Issue in the International Realm

The rapid development of cyberspace has drastically changed the international legal and security scenario to such an extent that international law is faced with the need to address issues which were mostly unpredictable when the core principles of international law were being formulated. Starting out as a means of information dissemination and academic cooperation, cyberspace has developed into an essential component in the management of state affairs, international business, finance, military activity, health care, and diplomacy (Schmitt, 2021). As noted by the International Telecommunication Union (ITU, 2023), over two-thirds of the world's population currently have Internet access, showing how important digital connectivity has become in modern society. With governments digitizing their state activities, cyber vulnerabilities pose not only a danger to the security of individual states but also to international peace and economy (Shackelford, 2014). The importance of cyberspace as a tool of strategy has grown immensely during the last two decades. Cyber actions have been incorporated into statecraft, allowing states to achieve political, military, economic, and intelligence goals without using conventional weaponry (Nye, 2017). Unlike regular military actions, which need physical presence and can be traced easily, cyber actions can be done remotely, anonymously, and at lower costs, but result in effects that go beyond the territorial borders of the state in question (Rid & Buchanan, 2015). Such advantages have encouraged the use of cyberspace by both state and non-state actors for espionage, sabotage,

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

disinformation campaign, IP theft, and attacks on critical infrastructures (Healey, 2013). Thus, cyberspace has turned out to be the fifth operational domain besides the land, sea, air, and outer space domains, which is recognized by various states and military alliances such as NATO (2016).

The growing instances of cyber threats have shown once again that cyber operations are able to bring about the same results as conventional military actions. The distributed denial-of-service (DDoS) attacks on Estonia in 2007 were able to disrupt the operation of banks, the functioning of websites of the Estonian government, and its communication system, showing that the use of cyber operations is capable of creating tangible problems for states heavily dependent on digital technologies (Ottis, 2008). In a similar vein, the Stuxnet computer virus discovered in 2010 was able to cause material damage to Iran's nuclear centrifuges, thus proving that cyber operations are not limited only to the realm of cyberspace (Langner, 2013). Recent examples include, among others, the SolarWinds supply chain attack and ransomware attacks on critical infrastructure. They serve to show the growing complexity of the cyber threat and its ability to endanger economic security and public administration (Schmitt, 2021).

Unlike other international regions regulated by international law, cyberspace does not adhere to the territoriality of jurisdiction. Milliseconds are all it takes to communicate across many jurisdictions. Cloud computing and data processing require infrastructures dispersed across several countries (Hathaway et al., 2012). Furthermore, cyberspace operations may be carried out with ease using decentralized infrastructure, privately managed networks, and anonymity techniques, making it difficult to identify the attackers and their point of origin. In spite of such specific characteristics inherent to cyberspace, it should be noted that the international community has not accepted any idea about cyberspace being a place free from law. On the contrary, it was increasingly recognized that the principles of international law continue to apply to cyber operations. Indeed, it has been clearly stated by the UN Group of Governmental Experts that international law as well as the Charter of the United Nations regulates the behavior of states in using ICTs (United Nations, 2013). Such an approach was confirmed again in the UN GGE Consensus Report of 2015 where it was underlined that the application of international law is crucial for ensuring peace, stability, and security in cyberspace (United Nations, 2015). Recently, the same approach to cyberspace was taken by the United Nations Open-Ended Working Group which stressed that international law sets norms of state behavior in cyberspace while supporting CBMs and international cooperation (United Nations, 2021).

The rising frequency of cyber-related events has further shown that cyber activities can cause repercussions which rival those of conventional military operations. The DDoS attack on Estonia in 2007 paralyzed banking operations, governmental websites, and communication networks, and showed how vulnerable digitally reliant countries can be to coordinated cyber attacks (Ottis, 2008). Likewise, the discovery of the Stuxnet worm in 2010 resulted in damage to Iran's nuclear enrichment program, demonstrating the ability of cyber operations to cause tangible damage outside of the cyber realm (Langner, 2013).

In more recent times, events like the SolarWinds cyber-attack and ransomware attacks on critical infrastructure have demonstrated the growing complexities of cyber threats and their ability to threaten economic security and governance. The lack of boundaries is what distinguishes cyberspace from all other conventional realms. It should be recognized that the Internet is characterized by information traveling across many jurisdictions in milliseconds, and that data processing and storage may occur using infrastructure dispersed throughout multiple nations (Hathaway et al., 2012). Furthermore, it may be hard to track down the origin of a cyberattack and identify the perpetrators due to the use of private networks, dispersed systems, and anonymization technologies.

This position has received much support from academic literature. In his work, Schmitt (2017) claims that the advent of any kind of technology does not make previously existing legal principles outdated; instead, the principles of international law need to be interpreted based on the advent of technology, unless the international community decides to develop new legal norms. Hollis (2021) claims that due to the flexibility

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

that exists within international law, principles of international law can develop in tandem with emerging technologies. However, there is still much debate among scholars about how these principles need to be interpreted in cyberspace (Efrony & Shany, 2018). These disputes demonstrate that the main question in international cyber law today is not whether international law applies in cyberspace, but rather how its provisions may be interpreted and implemented in the context of a society that is becoming more technologically advanced and linked. A greater emphasis has been placed on how the UN Charter, customary international law, court rulings, state practice, and initiatives like the Tallinn Manual 2.0 may be read in cyberspace due to the absence of an international agreement regulating inter-state cyber operations. Studying the sources of international law that apply in cyberspace is crucial.

2.2 Sources of International Law Governing Cyberspace

While cyberspace continues to evolve at an ever-increasing pace, and the nature of cyber threats becomes increasingly complex, there is still no multilateral treaty dealing solely with the behavior of states in cyberspace. As a result, the regulation of cyber operations will necessarily be based on the use of those sources of international law that are enumerated under Article 38(1) of the Statute of the International Court of Justice (ICJ). The sources include international conventions, customary international law, general principles of law, judicial decisions, and the works of prominent publicists (Statute of the International Court of Justice, 1945). It is through the use of these sources of international law that states evaluate the legality of cyber operations and derive their rights and obligations arising out of such cyber operations. The Charter of the United Nations is still the primary treaty governing international relations in cyberspace. Even though the treaty was developed many years ago, before the existence of the Internet, the main tenets , including sovereign equality as provided for by Article 2(1), non-use or threat of use of force as per Article 2(4), peaceful settlement of disputes as per Article 2(3) and inherent right of self-defence as provided for by Article 51, continue to govern the conduct of states regardless of the means used (United Nations, 1945). According to the UN Group of Governmental Experts, the Charter also covers the application of ICT by states, thus negating the view that cyberspace is outside the reach of international laws (United Nations, 2015). This has been further confirmed by the OEWG, which continues to recognize the Charter as the bedrock of cyber governance (United Nations, 2021).

Apart from the laws of treaties, customary international law forms an important aspect in the regulation of cyberspace. According to custom international law, rules are developed through persistent state practice coupled with the opinio juris, which is the conviction that such actions are taken as part of a legal obligation (North Sea Continental Shelf Cases, 1969). Since the development of cyber technologies occurs at a much faster rate compared to the processes involved in making treaties, custom international law has become increasingly important in solving problems that are not covered by any existing treaty law (Roscini, 2014). Principles like sovereignty, non-intervention, due diligence, state responsibility, and the prohibition of use of force have thus been applied in cyber operations via customary international law. However, determination of consistent state practice in the cyber space is difficult due to lack of transparency regarding cyber operations as well as unwillingness of states to make known their offensive cyber technologies (Efrony & Shany, 2018). The principles of international law further regulate cyberspace by addressing the gaps that exist in terms of treaty and customary laws. Principles such as good faith, necessity, proportionality, and due diligence have always been the guiding principles of interstate behavior, and these principles help interpret legal obligations in relation to the cyber operations. The principle of due diligence has grown in relevance when it comes to addressing the state responsibilities of preventing cyber operations initiated from the state territory to cause serious damage to other states. However, judicial pronouncements on legal issues are not binding sources of international law outside the disputing parties, but they offer some important guidelines for interpretation of international law in the cyber domain.

Decisions from the International Court of Justice, specifically from cases like Corfu Channel (1949), Military and Paramilitary Activities in and against Nicaragua (1986), and Oil Platforms (2003), have had a major impact on the contemporary discourse on issues such as sovereignty, non-intervention, use of force, and state responsibility (International Court of Justice, 1949; International Court of Justice, 1986; International Court

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

of Justice, 2003). Notwithstanding that the aforementioned cases did not concern cyber operations, the principles developed by the court continue to be relevant in scholarly and governmental discourse on international law in the cyber domain (Roscini, 2014). Likewise, UN GGE and OEWG report publications have made important contributions towards the development of cyber norms on an international level. Although these reports do not impose any legal obligations on states, they express a growing agreement about the responsible behavior of states in cyberspace and help build confidence-building measures and cooperation among states to decrease the likelihood of inter-state conflict (United Nations, 2015; United Nations, 2021). The tendency of increasingly using soft-law tools demonstrates the dynamic nature of international cyber governance, since non-binding norms often affect state practice and lead to the development of international customary law (Hollis, 2021).

In summary, the above discussion of the various sources proves that regulation of cyberspace is not fragmented and that there is law in cyberspace after all. Contemporary regulation of cyber does not necessarily need an entirely new body of international law, but rather requires an interpretation of the principles of international law in the context of the dynamic technological setting. The real problem with contemporary international cyber law is not lack of relevant law but achieving more coherence and consensus in its interpretation. Such interpretation becomes apparent especially when dealing with the principle of sovereignty, which is one of the most controversial aspects of international cyber law.

2.3 The Development of International Cyber Norms

The quick emergence of cyberspace has been much faster than the creation of international treaties governing cyber operations. To address the issue, states and international organizations have been increasingly turning to the formation of international norms of conduct in cyberspace in order to promote responsible conduct, prevent international conflicts, and improve cybersecurity on a global level (Tsagourias & Buchan, 2021). Contrary to treaty provisions, these norms of conduct often lack the binding nature; nevertheless, they have gained an increasing amount of influence on the practice of states, interpretation of international law, and consensus-building on the application of international law in cyberspace. This organization has been one of the pioneers of these normative changes. The United Nations created the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) in 2004 to assess the impact of ICTs from a security perspective and to develop ways of increasing peace and stability in the international realm (United Nations, 2004).

The creation of the UNGGE was indicative of a rising international concern that cyber activities could have an adverse effect on both national security and international relations. The important milestone was accomplished by the UNGGE Consensus Report in 2013 when it stated unambiguously that the international law in place applies to the actions of the states in cyberspace, including the UN Charter (United Nations, 2013). It meant that for the first time there was the official agreement between the major cyber powers on the application of the international law in cyberspace and refuted the previous views that cyberspace was a legal black hole. The final substantive report by the 2021 OEWG affirmed that international law, specifically the United Nations Charter, will remain the framework within which the behavior of states in cyberspace will be regulated (United Nations, 2021).

Furthermore, the need for confidence-building measures, capacity building, information sharing, and cooperation among states was recognized as a means of minimizing any risks of cyber warfare. In addition, the need to boost the resilience of states against cyber threats and promote transparency and dialogues on the interpretation of international law was emphasized (United Nations, 2021). Despite a lack of agreement on some issues, the OEWG has greatly increased international involvement and strengthened the validity of multilateral deliberations. In addition to UN initiatives, some regional and multi-stakeholder initiatives have also made contributions to the formulation of international cyber norms. The Convention on Cybercrime adopted by the Council of Europe in 2001 is currently the sole legally binding instrument in the international framework that addresses issues related to cybercrime and has immensely facilitated international cooperation

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

in criminal investigations relating to computer-based crimes (Council of Europe, 2001). Though the prime goal of the Convention is not to regulate interstate cyber activities but rather harmonize national criminal laws, the Convention illustrates the role of international legal cooperation in the sphere of cyber threats. In addition to this, more recent initiatives like the Paris Call for Trust and Security in Cyberspace (2018) have also increased efforts to ensure that states, international organizations, private firms, and civil society work towards common goals that help promote stability and security in cyberspace (Paris Call, 2018). Even though participation is voluntary, it is a clear indicator of the realization that cyber governance cannot be accomplished through the traditional legal mechanism between states, rather collaboration among different stakeholders is necessary.

Taking into consideration the progressive nature of the formation of international norms as they relate to the cyber realm, the evolution of international cyber governance happens through international treaties, customary international law, soft law, expert opinion, and practice of states. Yet, there remain some aspects of international law as they relate to cyber governance principles that raise issues about their interpretation, in particular issues related to sovereignty, non-interference, attribution, and the use of force. The problem arises here, and it is necessary to talk about it, this is the examination of the principles that guide state actions in cyberspace. This principle will be examined in this part of the study as it is the basis of international cyber law.

FUNDAMENTAL PRINCIPLES OF INTERNATIONAL LAW GOVERNING CYBERSPACE

The rising involvement of cyberspace in the functioning of governments, military, finances and infrastructures has highlighted the importance of international legal principles in the regulation of the state activity in the cyber space. Although cyberspace raises new technological challenges, it cannot be exempt from international law. On the contrary, international legal principles still regulate state activity, but their interpretation and application should be adjusted to specific conditions of cyber operations (Schmitt, 2021). The UN has already stated on numerous occasions that international law, especially the Charter of the UN, continues to be relevant for ICTs of states (United Nations, 2015; United Nations, 2021). Thus, the regulation of cyber activity is mostly dependent on public international law principles, such as sovereignty, non-intervention, prohibition of the use of force, the right of self-defence and state responsibility.

3.1 The Principle of Sovereignty in Cyberspace

Sovereignty continues to be the bedrock of the international legal system as the legal right of a state to have exclusive jurisdiction within its territory, institutions, and people without interference from outside (Shaw, 2021). Sovereignty is an explicitly stated principle in Article 2(1) of the Charter of the United Nations as the sovereign equality of all the Member States (United Nations, 1945). Traditionally, sovereignty was viewed as something that was territorial in nature, but due to the digitization of state activities, sovereignty also holds significance for cyberspace. The International Court of Justice (ICJ) always regarded the concept of sovereignty as a cornerstone of international law. According to the Court, respect for the sovereignty of a state's territory is an essential foundation of international relations (ICJ, 1949).

In the same vein, in the case of Nicaragua, the ICJ reiterated that every state has the right to manage its internal affairs without any kind of external interference (ICJ, 1986). However, these cases occurred before the advent of the internet and are still relevant in the regulation of cyber operations (Roscini, 2014). The main point of discussion here is about whether sovereignty is just a general principle or can be seen as a distinct rule which can be breached by cyber actions. In this regard, Tallinn Manual 2.0 holds that cyber operations causing destruction to physical objects, disruption of functionalities of cyber infrastructure, or interference with inherently governmental functions can violate sovereignty even in the absence of use of force (Schmitt, 2017). This view has been supported by various countries including France, the Netherlands, Estonia, Australia, and Finland who recognize sovereignty as an independent legal duty in cyberspace. On the other hand, the United Kingdom has opted for a more restricted interpretation, arguing that the concept of sovereignty operates mainly as a principle from which other obligations such as non-intervention and prohibition of the use of force are

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

derived (UK Attorney General, 2018). Under this perspective, not all unauthorized cyber activity necessarily amounts to a violation of international law. The difference above exemplifies the uncertainty that still prevails as far as the legal standard necessary for committing an act against sovereignty in cyberspace is concerned.

3.2 The Principle of Non-Intervention

Non-intervention is another aspect which is closely associated with the concept of sovereignty since it bars the states from coercively intervening in the affairs of another state which fall under its domestic jurisdiction. Non-intervention principle can be seen as enshrined in Article 2(7) of the Charter of the United Nations and has also been recognized as a part of customary international law by the International Court of Justice (United Nations, 1945; ICJ, 1986).

In the case of Nicaragua, the Court stated that intervention without coercion involves interference in the sphere in which the states have the right to take decisions freely. The applicability of the above principle to cyberspace has been a source of extensive scholarly controversy. The use of cyber tools to sway an election, affect the opinions of citizens through the use of propaganda, influence government decision-making, or affect the operation of democratic institutions could be deemed an illegitimate interference if such operations involved coercion that is aimed at another state's sovereign decisions (Tsagourias & Buchan, 2021). For instance, electoral interference in cyberspace has been a topic of concern since it is linked to the threat to democratic governance and political autonomy, especially from foreign states. However, the determination of whether there is coercion in cyberspace is not an easy process. Although it is easier to label any activity in cyberspace that leads to the disruption of government systems as an intervention, influence campaigns carried out through social media and online propaganda have been classified as a gray area in law since they rely more on persuasion than coercion.

3.3 The Prohibition of the Use of Force

Whether a cyber attack qualifies as an unlawful use of force is mainly dependent on the scale and impact of such action rather than the tools used. In the Tallinn Manual 2.0, cyber operations resulting in physical damage, injury, or interference in critical infrastructure can be classified as satisfying the criterion of the use of force as stated in Article 2(4). This has been illustrated by the Stuxnet attack in Iran where there was physical damage of the centrifuge through computer malware (Langner, 2013). Likewise, attacks on power supply systems, health facilities, transport systems, and military communication systems may result in similar impacts as an armed attack. However, there are various cyber operations including economic espionage, website defacement, temporary denial of service and confidential information theft that do not cross the threshold of use of force because of their possible serious economic impact (Nye, 2017). This is one example of the necessity of the assessment of the seriousness and impact of cyber operations on their legal characterisation.

3.4 The Right to Self-Defence

However, when the cyber operation amounts to an armed attack, then the injured state has the right to self-defense in accordance with Article 51 of the UN Charter (United Nations, 1945). It should be noted that the International Court of Justice made a difference between an illegitimate use of force and an armed attack, meaning that the former can lead to the right of self-defense. Such a differentiation is very important in cyberspace because many attacks in this area result in great disruption but no damage to the physical objects. It is widely accepted that cyber attacks which cause significant physical damage, death, or serious destruction to critical infrastructure can be considered an armed attack, thus enabling resort to Article 51 (Dinstein, 2021; Schmitt, 2017). At the same time, cyber attacks involving hacking and stealing of information, ransomware attacks, or short-term disruption of services do not amount to an armed attack. Even if self-defence can be rightfully resorted to, any use of force should still meet the criteria of necessity and proportionality (Dinstein, 2021).

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

3.5 State Responsibility and Attribution

The successful use of international law in the cyber domain is reliant on the capacity to identify those parties responsible for carrying out cyber operations. The responsibility of states to internationally wrongful acts under Article 1 of the ARSIWA holds a state liable for any action that can be attributed to them and which violates its international obligations (ILC, 2001). Attribution thus poses one of the toughest challenges in cyber governance today. As opposed to conventional military activities, cyber attacks are usually carried out through proxy actors, hacker groups, botnets, or infected infrastructure present in the third states, which hides the actual identity of the state conducting such attacks (Rid & Buchanan, 2015).

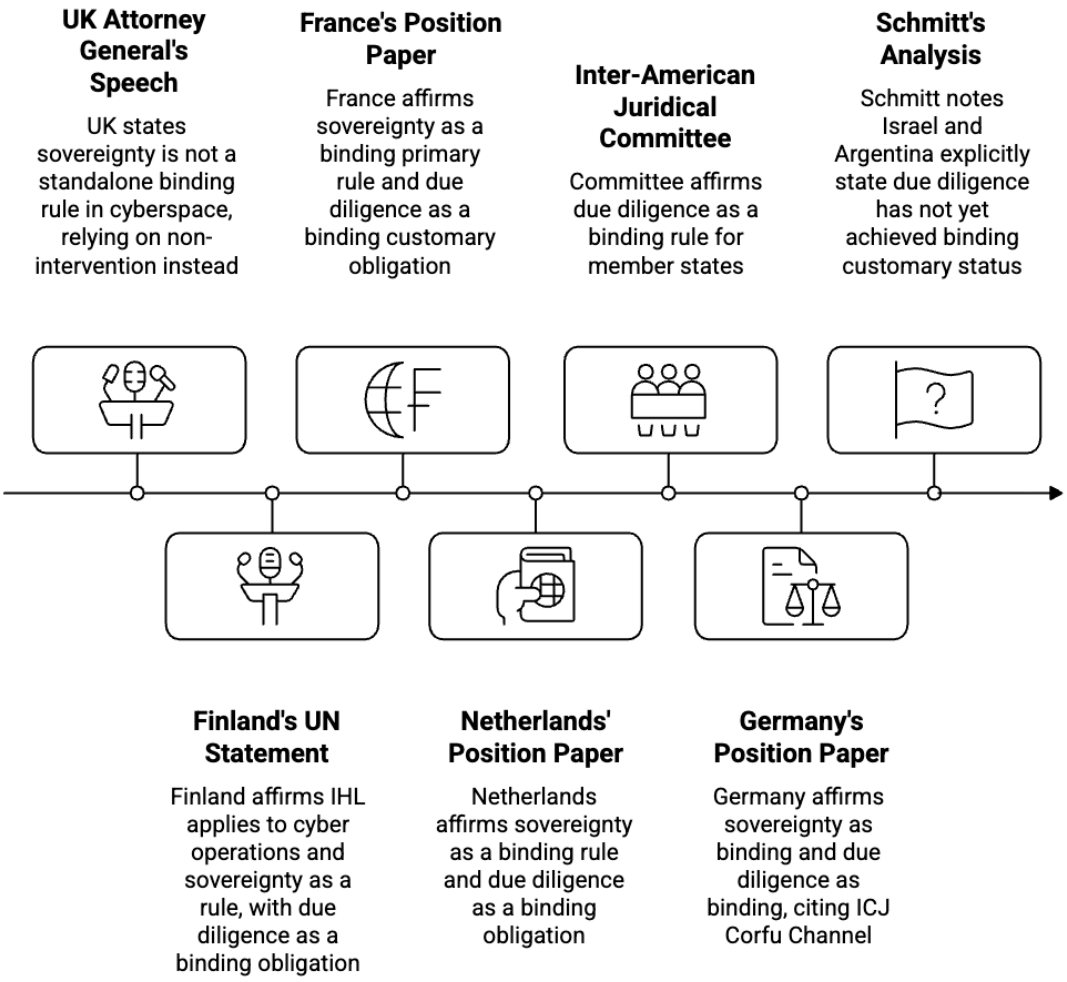

Table 2: Selected State Positions on the Legal Status of Sovereignty and Due Diligence in Cyberspace
(**Source:** United Nations Institute for Disarmament Research. (2023). Due Diligence in Cyberspace: Normative Expectations of Reciprocal Protection of International Legal Rights; United Nations Institute for Disarmament Research. (2026). Due Diligence in Early Practice, the International Law Commission Agenda and Cyberspace; NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). International Cyber Law: Interactive Toolkit)

A technical attribution is not enough to prove the legality of the act since proving responsibility in accordance with the norms of international law requires demonstrating a link between the act and the state. The ICJ employed the "effective control" standard in the Nicaragua case, while the ICTY developed the wider "overall control" standard in the Tadić case (ICJ, 1986; Prosecutor v. Tadić, 1999). Whether these criteria can be applied in cyberspace remains a point of academic discussion. Due diligence comes hand-in-hand with attribution because it calls for states to take action within their jurisdiction and cyberspace so as to avoid causing serious damage to other states when they are aware and capable of doing so. While more states have

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

become supportive of due diligence in cyberspace, it still remains contentious as to whether or not there is a rule of customary international law emerging in the area (Efrony & Shany, 2018). However, improving mechanisms for attribution and international cooperation is vital in this context. The above-mentioned principles, taken together, clearly illustrate that there is already a considerable body of international law covering cyberspace. Nonetheless, problems such as different state practices, technological developments, and questions of attribution persist and impede the uniform application of these principles. Such an observation points to the necessity to analyze the concrete hurdles in the application of international law in cyberspace, and this is done in the subsequent section.

CONTEMPORARY CHALLENGES IN THE APPLICATION OF INTERNATIONAL LAW TO CYBERSPACE

In spite of the fact that it has become common ground that the current set of principles of international law applies to cyberspace, implementing them poses several obstacles from a legal, technical, and political standpoint. While in the case of other arenas of conflict it is relatively straightforward to ensure compliance with international legal obligations due to the fact that cyberspace is marked by anonymity, decentralization, speed, and lack of territorial demarcations (Schmitt, 2021), it can be said that in spite of the existence of the Charter of the United Nations, customary international law, and the law of state responsibility that offer a framework for regulating cyber operations, the specificities of cyber operations often obstruct its consistent implementation (Tsagourias & Buchan, 2021).

4.1 The Attribution Problem

The problem of accurate attribution of cyber operations in order to apply international law to cyberspace is one of the greatest challenges in using international law in cyberspace. The difference between the conventional military operation and cyber operation is that cyber operation can take place from a remote computer that is controlled by means of the compromised server, virtual private network, botnet, or some other third-party equipment across different jurisdictions in order not to disclose the identity of the person who performed the operation (Rid & Buchanan, 2015). This aspect adds even more complexity when discussing the matter. Technical attribution implies establishing the source of malicious cyber activity by conducting a forensic investigation; legal attribution involves providing enough evidence that such behavior can be attributed to the state in accordance with the principles of international law (International Law Commission, 2001). In accordance with ARSIWA, internationally wrongful acts have to be attributed to the state via its organs, agents, or any other entities operating under the control and direction of the state in order to invoke international responsibility (ILC, 2001).

In addition to the uncertainties mentioned above, judicial decision-making has created various criteria for attribution, adding further confusion. For example, in the case of Military and Paramilitary Activities in and against Nicaragua, the International Court of Justice introduced the criterion of “effective control,” whereby responsibility can be attributed only if a state has direct control over particular actions carried out by non-state entities (ICJ, 1986). On the contrary, in the case of Prosecutor v. Tadić, the International Criminal Tribunal for the Former Yugoslavia introduced the criterion of “overall control,” implying less involvement from the side of the state (ICTY, 1999). The application of such criteria to cyber operations is still disputable, as cyber-attacks are often committed by loosely organised hacker collectives or proxies. The above-mentioned challenges can be observed from recent cyber events. The SolarWinds software supply chain attack that occurred in 2020 was carried out against many governmental entities as well as businesses around the world. While some countries have already attributed the attacks to people belonging to the Russian SVR, such attribution was done primarily based on intelligence reports as opposed to public legal proof (CISA, 2021). The same is true for the Microsoft Exchange server attacks carried out by Chinese state actors and resulting in many diplomatic reactions despite ongoing controversy concerning international law's threshold of proof (United States Department of Justice, 2021).

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

4.2 Cyber Operations Conducted by Non-State Actors

One other notable problem revolves around the growing influence of non-state actors in the cyberspace domain. In contrast to conventional warfare scenarios where state militaries usually carry out their military activities, cyberspace features the presence of criminal organizations, terrorists, hacktivists, patriots, and cyber contractors in their activities (Shackelford, 2014). Such non-state actors often boast advanced technological abilities that enable them to destabilize the functioning of government and critical infrastructure without the intervention of the state. Ransomware groups like REvil, Conti, and LockBit show how cybercrime organizations have become increasingly capable of causing substantial economic harm to governments as well as private institutions (Europol, 2023). Similarly, hacktivist organizations like Anonymous have shown that they are capable of conducting political cyber operations against governmental websites and public infrastructure. Although such groups do not fall under international law in the same way as states, their actions usually cause international legal implications for states that support or sanction them in some way (ILC, 2001). There is another issue that emerges as a consequence of the growing practice of using proxies. In some cases, states intentionally use hacker groups for conducting cyber activities in such a way that the state's role is not clearly identified (Rid & Buchanan, 2015). This complicates the process of attribution and makes existing legal procedures regarding the liability of the state ineffective. With cyber conflict becoming increasingly hybrid in nature, it becomes increasingly hard to distinguish what is public and what is private.

4.3 Jurisdictional and Enforcement Challenges

Cyberspace is another realm where there are numerous issues related to jurisdiction, since actions in cyberspace tend to transcend national boundaries. Cyber operations can take place in one state and go through servers in other states, have victims in various jurisdictions and be carried out using cloud services located in different continents (Hathaway et al., 2012). The transnational nature of cyberspace poses difficulties in deciding what state has the jurisdiction to deal with certain cyber activities. Differences in national legislation cause overlapping claims to jurisdiction while differences in domestic legal frameworks hinder efficient collaboration internationally. Mutual legal assistance mechanisms are usually ineffective in addressing rapidly changing cyber events since they take too much time and thus enable the criminals to erase all traces of the crime or even move their infrastructure to another jurisdiction (Council of Europe, 2001). In addition to this, there are many states that do not wish to provide access to electronic evidence across borders. The failure to achieve universal membership to the international cybercrime agreements also adds another layer to these problems. While the Budapest Cybercrime Convention has played a big role in increasing international cooperation between its parties, there is no doubt that the effectiveness of the convention has been hampered by the fact that key cyberpowers are not party to it (Council of Europe, 2001).

4.4 Rapid Technological Developments

The rate at which technology advances is often faster than that of international laws to respond adequately. There have been several emerging technologies including artificial intelligence (AI), machine learning, quantum computing, Internet of Things (IoT) and autonomous cyber capabilities, all of which have greatly increased opportunities and challenges presented by cyberspace. AI-powered cyber weapons are capable of quickly detecting weaknesses, launching automated phishing attacks, creating advanced malware and performing cyber operations without much human interaction (Brundage et al., 2018). In a similar way, the growth of IoT devices that are connected to each other has considerably expanded the global cyber attack surface. Many infrastructures, such as healthcare systems, transport, industrial control systems, and energy infrastructures, become more and more dependent on connected digital devices that often lack sufficient cyber security measures (ENISA, 2023). Thus, vulnerabilities emerge, allowing cyber operations that can cause disruptions at a large scale. The emergence of quantum computing poses another set of legal challenges. The future quantum technologies might pose threats to existing cryptographic systems, which will completely change the ratio of cybersecurity and cyber vulnerability (National Institute of Standards and Technology, 2022). It is obvious that many security challenges of these rapidly evolving technologies have not been considered by the current legal frameworks yet.

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

4.5 Fragmentation of State Practice

The last important barrier to the evolution of international cyber law is the lack of uniform practice of states. It is accepted by many states that international law already in its current form applies to cyberspace. Nevertheless, the understanding of several important principles of international law is very different among states – the principles of sovereignty, due diligence, countermeasures and the threshold of the use of force. For example, France and Netherlands interpret the principle of sovereignty as a distinct principle of international law applicable to cyber operations, while the position of the UK is more limited (French Ministry of the Armed Forces, 2019; Government of the Netherlands, 2019; UK Attorney General, 2018). The same can be stated about due diligence and countermeasures. The fragmented nature of such international legal obligations poses difficulties in developing customary international law and leads to uncertainties in interpretation. Without further unification of practice and opinio juris, the interpretation of international legal obligations in cyberspace will most likely be controversial, leading to lack of predictability and higher chances of misunderstanding between states. Overall, it can be concluded that the main issues related to the applicability of international law to cyberspace do not lie in the lack of legal norms, but rather in unique features of cyber operations. The issues of attribution, participation of non-state actors, complex jurisdiction, innovative character of technologies, and diverging state practice still make it difficult to apply international legal rules in cyberspace. Such issues require higher levels of international cooperation and legal development, which form the foundation of recommendations provided below.

STRENGTHENING THE INTERNATIONAL LEGAL FRAMEWORK FOR CYBERSPACE

The fast development of cyberspace has shown that even though the current principles of international law serve as an important legal basis, some deficiencies still exist in its application. The transnational character of the cyber sphere, as well as the inconsistency of state behavior and the development of new technologies, has made it unclear how to regulate cyber operations (Hathaway et al., 2012). Thus, the task should be not to replace the current principles of international law but rather to clarify them and improve international cooperation.

5.1 Promoting International Legal Harmonization

One of the top priorities is the creation of a better understanding about the use of international law in relation to cyber space. While there is an understanding among the states that international law applies to cyber space, there remains a dispute about certain topics like sovereignty, due diligence, and the threshold for use of force (Jensen, 2015). A harmonization could be achieved through dialogues at the United Nations and other regional organizations and forums. Even though it may be difficult to negotiate a cyber treaty, it will be beneficial for creating clarity (Hollis, 2023).

5.2 Strengthening International Cooperation

Due to their inherent global character, cyber security challenges cannot be resolved at the national level. Therefore, it is essential to increase collaboration through cyber exercises, information exchanges, and incident response coordination systems (Nye, 2017). In particular, regional cybersecurity agencies and international organizations like the UN, NATO, and INTERPOL must continue to strive for greater state-to-state collaboration and increased cyber resilience. It will contribute to the development of shared norms for nations to behave responsibly in cyberspace and foster trust (Klimburg, 2017).

5.3 Improving Attribution and Accountability

The efficiency of international law, to a large extent, is determined by the possibility of attributing actions in cyberspace to someone. The problem with that is that the complexity of technology and the employment of proxies complicate the process of attribution (Lindsay, 2015). Therefore, states need to develop more sophisticated cyber forensics and enhance cooperation between CERTs and law enforcement agencies. International acceptance of the standards of evidence in cyber investigations would increase accountability for internationally wrongful cyber activities (Buchan, 2016).

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

5.4 Enhancing Capacity Building

Regarding cyber security, there are significant differences across countries, particularly between industrialized and poor ones. Most countries still lack the knowledge, resources, and laws necessary to combat cyberthreats (Global Forum on Cyber Expertise, 2021). In this regard, the provision of technical assistance, training, and legislative measures must be given top priority in any international cyber capacity development. In addition to helping particular nations, such initiatives will foster stability in the global online ecosystem.

5.5 Ensuring the Protection of Human Rights

The process of improving cybersecurity needs to be in line with the state's international obligations regarding human rights. All measures taken by the state to respond to the threat posed by cyberspace need to adhere to the human rights of privacy, freedom of expression and access to information as provided by international human rights law (Kaye, 2019). The state needs to make sure that any forms of surveillance, data collection and cybersecurity measures satisfy legality, necessity and proportionality principles.

In conclusion, greater international collaboration, precise legal frameworks, effective attribution procedures, and greater funding for cybersecurity capacity building are all necessary for international cyber laws to be successful in the future. The international community must work together to ensure that international rules can maintain peace and security in cyberspace in light of the ongoing growth of cyber dangers brought about by new technological advancements.

CONCLUSION

The advent of cyberspace has completely changed the character of international relations through providing new chances for communication, economic growth, technology advancements, and connections around the globe. However, it has also created new problems related to laws and security, which go beyond conventional geographical limits and pose a challenge to the capacity of international law to adjust to changes. With an increasing reliance of states on digital technology for the purpose of governance, defense, business, and service provision, the stability and security of cyberspace have become key concerns. As has been shown in this paper, international law is not missing in cyberspace. On the contrary, the current system of international law, namely the Charter of the United Nations, customary international law, and the law of state responsibility, constitutes the main legal foundation for the regulation of states' behaviour in the cyber realm (United Nations, 1945). Such principles as sovereignty, non-intervention, prohibition of the use of force, self-defence, and state responsibility still remain applicable to cyber operations; however, the interpretation of them should be adjusted to the realities of cyberspace. In addition, international projects aimed at ensuring cybersecurity, such as UNGGE and OEWG initiatives, prove once again that the existing international law still regulates states' behaviour in cyberspace (United Nations, 2021). However, the research indicates that the application of legislative regulations, rather than their absence, is the primary issue. International law implementation is nonetheless hampered by attribution concerns, the expanding participation of non-state actors, jurisdictional challenges, disparate state practices, and the rapid advancement of information technology (Hathaway et al., 2012).

Even if the international community is becoming more interested in cyber governance, different interpretations of sovereignty, due diligence, and state use of force demonstrate that normative ambiguity still exists. The analysis goes further to show that efforts to bolster the international legal regime may not involve the creation of an entire new regime of international law but rather an increased focus on making clear existing principles of law, fostering consistency in state practice, facilitating international cooperation, improving attribution measures, and increasing cybersecurity capabilities. The dialogue within the United Nations and other multilateral institutions will be key in creating greater legal certainty and developing custom international law in cyberspace (Hollis, 2023).

Finally, the future of international cyber governance will rely on the readiness of nations to work together in order to tackle shared security threats but with regard to international law principles. With the continuous

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

evolution of technology influencing the international legal environment, it is important to develop a consistent legal framework that will allow for the maintenance of peace, security, and stability in cyberspace. A proper combination of legal certainty, international cooperation, technological advancement, and protection of human rights will allow for the provision of a secure, open, and rule-based cyberspace.

REFERENCES

1. Buchan, R. (2016). Cyber attacks: Unravelling the international law of attribution. *Journal of Conflict and Security Law, 21*(2), 399–423.
2. Council of Europe. (2001). *Convention on Cybercrime (ETS No. 185).* https://www.coe.int/en/web/cybercrime/the-budapest-convention
3. Dinstein, Y. (2021). *War, aggression and self-defence* (8th ed.). Cambridge University Press.
4. Efrony, D., & Shany, Y. (2018). A rule book on the shelf? *Tallinn Manual 2.0* on cyber operations and subsequent state practice. *American Journal of International Law, 112*(4), 583–657. https://doi.org/10.1017/ajil.2018.86
5. Global Forum on Cyber Expertise. (2021). *Global cybersecurity capacity building report.* https://thegfce.org
6. Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review, 100*(4), 817–885. https://www.jstor.org/stable/23249948
7. Healey, J. (2013). *A fierce domain: Conflict in cyberspace, 1986–2012.* Cyber Conflict Studies Association.
8. Hollis, D. B. (2021). The influence of war; the war for influence. In N. Tsagourias & R. Buchan (Eds.), *Research handbook on international law and cyberspace* (pp. xx–xx). Edward Elgar Publishing.
9. Hollis, D. B. (Ed.). (2023). *The Oxford handbook of international law and cyberspace.* Oxford University Press.
10. International Court of Justice. (1949). *Corfu Channel (United Kingdom v. Albania), Merits, Judgment.* I.C.J. Reports 1949, 4.
11. International Court of Justice. (1969). *North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. Netherlands), Judgment.* I.C.J. Reports 1969, 3.
12. 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, 14.
13. International Court of Justice. (2003). *Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment.* I.C.J. Reports 2003, 161.
14. International Law Commission. (2001). *Draft articles on responsibility of States for internationally wrongful acts, with commentaries.* In *Yearbook of the International Law Commission, 2001* (Vol. II, Part Two). United Nations.
15. International Telecommunication Union. (2023). *Facts and figures 2023.* https://www.itu.int
16. Jensen, E. T. (2015). The Tallinn Manual 2.0: Highlights and insights. *Georgetown Journal of International Law, 46*(3), 735–778.
17. Kaye, D. (2019). *Speech police: The global struggle to govern the internet.* Columbia Global Reports.
18. Klimburg, A. (Ed.). (2017). *National cybersecurity framework manual.* NATO Cooperative Cyber Defence Centre of Excellence.
19. Langner, R. (2013). *To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve.* The Langner Group.
20. Lindsay, J. R. (2015). Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity, 1*(1), 53–67.
21. NATO. (2016). *Warsaw Summit Communiqué.* https://www.nato.int
22. Nye, J. S., Jr. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266
23. Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In *Proceedings of the 7th European Conference on Information Warfare and Security* (pp.

DOI: 10.22178/acta.27.3.1

ISSN: 2178-7727

163–168).
24. Paris Call. (2018). *Paris Call for Trust and Security in Cyberspace.* https://pariscall.international
25. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382
26. Roscini, M. (2014). *Cyber operations and the use of force in international law.* Oxford University Press.
27. Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations.* Cambridge University Press.
28. Schmitt, M. N. (2021). *Advanced introduction to international cyber law.* Edward Elgar Publishing.
29. Schmitt, M. N., & Vihul, L. (2017). Respect for sovereignty in cyberspace. *Texas Law Review*, *95*(7), 1639–1670.
30. Shackelford, S. J. (2014). *Managing cyber attacks in international law, business, and relations: In search of cyber peace.* Cambridge University Press.
31. Statute of the International Court of Justice, June 26, 1945, 33 U.N.T.S. 993.
32. Tsagourias, N. (2015). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, *17*(2), 229–244.
33. Tsagourias, N., & Buchan, R. (Eds.). (2021). *Research handbook on international law and cyberspace.* Edward Elgar Publishing.
34. United Nations. (1945). *Charter of the United Nations.* https://www.un.org/en/about-us/un-charter
35. United Nations. (2004). *Developments in the field of information and telecommunications in the context of international security* (A/RES/58/32).
36. United Nations. (2013). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98). https://documents.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf
37. United Nations. (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174). https://documents.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf
38. United Nations. (2019). *Advancing responsible State behaviour in cyberspace in the context of international security* (A/RES/73/266).
39. United Nations. (2021). *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final substantive report* (A/75/816). https://documents.un.org/doc/UNDOC/GEN/N21/423/20/PDF/N2142320.pdf

DOI: 10.22178/acta.27.3.1