

Cyber Attacks under International Law



Hemis Maamar ^{1*}

¹ Faculty of Law and Political Science, Djilali Bounaama University of Khemis Miliana, Laboratory of Civil Status System, Algeria.

maamar.hemis@univ-dbkm.dz

Date of transmission: 23/09/ 2025, date of acceptance: 22/10/ 2025

Abstract:

Cyber-attacks represent one of the most pressing challenges facing international law in the digital era. They raise legal questions regarding their classification: should they be considered a use of force, an act of aggression, or merely a violation of state sovereignty? The issue also concerns the applicability of traditional principles of international law, such as non-intervention and the obligation not to allow one's territory to be used for hostile acts. Despite international efforts to establish norms governing cyberspace, the absence of a comprehensive treaty remains a major obstacle. Consequently, the debate continues on how to strike a balance between cybersecurity and the maintenance of international peace and security.

Keywords: Cyber Attacks, International Law, Cyberspace Governance, State Sovereignty, Use of Force.

* Hemis Maamar

Introduction

In recent decades, the world has witnessed an unprecedented technological revolution with the emergence of cyberspace as a new domain for communication, economy, and politics. However, this development has been accompanied by a notable increase in cyber attacks targeting states' critical infrastructures, including energy systems, hospitals, financial institutions, and elections. This has transformed cybersecurity into an issue of great sensitivity under international law. Such attacks raise a fundamental question regarding the extent to which they can be subjected to the rules of public international law and international humanitarian law, particularly in the absence of a comprehensive international convention regulating the digital domain (Schmitt, 2013, p. 21)

Cyberspace has increasingly become a new arena for human interaction and a theater where economic, political, and military interests of states and individuals intersect. With the advancement of information and communication technologies, cyber attacks have evolved from mere acts of sabotage with limited impact to transboundary threats that may affect critical infrastructures, disrupt government operations, and undermine international peace and security.

What makes cyber attacks the subject of broad legal debate is their dual nature: they may take the form of individual cybercrimes, or they may escalate to the level of "use of force" or even "armed attack" if they cause severe material damage, such as the **Stuxnet attack** on Iran's nuclear facilities in 2010 (Thomas Rid. **Cyber War Will Not Take Place. Oxford: Oxford University Press, 2013, P 47**), or if they widely disrupt a state's vital institutions, as in the case of **Estonia in 2007** (European Union, 2013, P 14)

Thus, studying these attacks under the lens of international law becomes crucial to understanding the scope of international responsibility, activating accountability mechanisms, and exploring clearer legal frameworks to regulate this new domain.

The importance of this topic lies in the following points:

- It clarifies the international legal framework through which cyber attacks can be classified.
- It helps understand the relationship between cyber operations and international law principles, such as the prohibition of the use of force, the principle of sovereignty, and non-intervention.
- It highlights the challenges faced by the international community in establishing state responsibility for cyber attacks (Oona A Hathaway and others , 2012, p. 830.)
- It opens the door for discussion on the need to draft a specialized international treaty for cybersecurity.

Cyber Attacks under International Law

Accordingly, the objectives of this research can be summarized as follows:

- To analyze the nature of cyber attacks and distinguish them from other cyber activities.
- To study the applicability of public international law and international humanitarian law to such attacks.
- To determine states' international responsibility for cyber attacks under the rules of attribution.
- To review major international and regional initiatives aimed at countering cyber threats.
- To provide practical recommendations to strengthen the international legal framework of cybersecurity.

Despite the tremendous technological progress, international law still faces major challenges in addressing cyber attacks, both in terms of their legal classification—whether as acts of aggression, terrorism, or transnational crimes—and in terms of determining international responsibility, given the difficulty of attributing them to specific states.

This raises a central research question:

To what extent can cyber attacks be considered as a use of force or an armed attack under international law, and what are the limits of state responsibility for such attacks in the absence of a comprehensive international cybersecurity framework?

To answer this question, this study relies on the descriptive-analytical method, through examining international legal texts (the UN Charter, international humanitarian law, and their relevant provisions regarding cyber attacks), and the comparative method, by comparing the positions of major states (United States, Russia, China) concerning the classification of cyber attacks.

It also employs the inductive method by analyzing practical cases (the Stuxnet attack on Iran in 2010 and the 2007 cyber attacks on Estonia) to extract how international law has dealt with these events. Accordingly, the study is structured as follows:

- Section 1: The Conceptual and Legal Framework of Cyber Attacks
- Section 2: Mechanisms of Response

Section 1: The Conceptual and Legal Framework of Cyber Attacks

Cyber-attacks have emerged as one of the most pressing challenges in the digital age, raising profound questions for international law. Understanding their conceptual foundations is crucial to defining their nature and scope. From a legal perspective, cyber-attacks intersect with principles of sovereignty, the prohibition of the use of force, and state responsibility. The absence of a comprehensive international treaty further complicates the regulation of cyberspace. This study seeks to clarify the conceptual and legal framework governing cyber-attacks, highlighting both challenges and prospects.

A : Defining Cyber Attacks and Distinguishing Them from Other Cyber Activities

Cyberspace is defined as “the global domain associated with computer networks and information infrastructure.” (Eneken, 2017, p)

Cyber attacks differ from mere acts of espionage or unauthorized access; they are understood as “any electronic activity that leads to the disruption, destruction, or weakening of the function of a system, network, or critical infrastructure.” (Oona A Hathaway and others, 2012, p. 832)

Actors in this domain are diverse: states pursuing political or military objectives, organized groups, private companies, or even individuals (hackers) (Schmitt, 2013, p. 21)

1 : Defining Cyber Attacks

Cyber attacks are:

Any hostile act carried out through cyberspace using technical tools (malware, viruses, denial-of-service attacks, intrusions...) with the aim of causing material, moral, or technical harm to information systems, networks, critical infrastructures, or governmental and private institutions (Ibid, p. 35)

Some literature has defined them as:

“The unlawful or unauthorized use of information systems and electronic communications that leads to their disruption, destruction, or interference with their vital functions.” (Al-Obaidi, 2020. p. 77.)

2 : Distinguishing Cyber Attacks from Other Cyber Activities

- **Cyber Attacks :**

- Aim to cause actual harm (material, functional, or security-related).
- Example: destroying a power grid, disrupting an air navigation system, hacking the Ministry of Defense's systems.
- Under international law, they may amount to the “use of force” or “armed attack” if their effects are comparable to conventional weapons.

Two major historical examples often cited:

- **The 2010 Stuxnet Attack**

Targeted Iran's nuclear program through a sophisticated malware that disrupted centrifuges at the Natanz facility. This is considered one of the first examples of using cyber capabilities to cause tangible material damage (destruction of sensitive equipment), akin to a traditional military act. It opened a wide debate on whether cyber attacks could be classified as “use of force” or even “armed attack” under Article 51 of the UN Charter (Falliere, O. Murchu, and Chien, 2011, pp. 6–15.)

- **The 2007 Estonia Cyber Attacks**

Considered the first major state-level cyber crisis, Estonia faced large-scale cyber attacks targeting its digital infrastructure (government institutions, parliament, banks, media). Although they did not result in direct material damage, they paralyzed state functions, sparking legal debate: should they be considered mere “electronic sabotage operations” or classified as “cyber aggression”? (Ottis, 2008, pp. 163–168.)

- **Other Cyber Operations or Activities (Cyber Operations / Activities):**

- May include cyber espionage, information gathering, surveillance, or online propaganda.
- Do not directly aim to destroy or disrupt but rather to gain strategic or informational advantage.
- Example: hacking the email of a Ministry of Foreign Affairs, or launching a disinformation campaign via social media.
- While such activities may be unlawful, they usually do not reach the level of “aggression.”

B : The International Legal Basis Governing Cyberspace

Despite the absence of a comprehensive international treaty, general principles of international law apply:

- **UN Charter**, Article 2(4) prohibits the use of force in international relations, while Article 51 enshrines the right of self-defense.
- **The principles of sovereignty and non-intervention**, whereby any cyber intrusion targeting another state's systems constitutes a violation of its sovereignty (Schmitt, 2013, p. 25)
- **International humanitarian law (IHL)** applies in cases of armed conflict, including cyber operations linked to such conflicts (Ibid, p 35)

Although cyberspace is a relatively new strategic domain, public international law remains the primary legal reference for its regulation.

1: The Principle of State Sovereignty and Non-Intervention

- **The Principle of State Sovereignty**
 - Applies to cyberspace, granting each state the right to control its information infrastructure and networks.
 - Any unauthorized intrusion or interference constitutes a violation of sovereignty (Ibid, p. 15)
 - The ICJ confirmed in the *Nicaragua v. United States* case that interference in the internal affairs of a state amounts to a breach of sovereignty International Court of Justice (ICJ), *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua ,1986, p. 14.)
- **The Principle of Non-Intervention**
 - Prohibits any state from interfering in another state's internal affairs via cyberspace, whether by influencing its electoral systems or destabilizing its political order.
 - This principle is derived from Article 2(7) of the UN Charter.

2 : The Prohibition of the Use of Force and International Humanitarian Law

- **The Prohibition of the Use of Force**
 - Article 2(4) of the UN Charter prohibits the threat or use of force against the territorial integrity or political independence of states.
 - This applies to cyberspace if cyber attacks cause effects equivalent to conventional weapons (destruction of facilities, disabling of defense systems, human casualties) (op cit , p. 47)

- **International Humanitarian Law (IHL)**

- If cyber attacks reach the level of armed conflict, IHL rules apply.
- Cyber operations must respect the principles of:
 - **Distinction** (between civilian and military targets).
 - **Proportionality** (ensuring civilian losses do not outweigh the anticipated military advantage) (International Committee of the Red Cross (ICRC), 2019, P 5)

3 : The Right of Self-Defense and Specialized Treaties and Agreements

- **The Right of Self-Defense**

- Under Article 51 of the UN Charter, if cyber attacks reach the level of “armed attack,” the affected state may exercise self-defense.
- Example: attacks that disable electricity grids or hospitals causing deaths.

- **Specialized Treaties and Agreements**

- **The Budapest Convention on Cybercrime (2001):** the most significant international framework for addressing cybercrime (Council of Europe, **Convention on Cybercrime (Budapest Convention)**, 2001., P 03)
- **UN General Assembly Resolutions:** such as Resolution A/RES/73/27 (2018) on “Developments in the Field of Information and Telecommunications in the Context of International Security.”

Section 2 : Mechanisms of Confrontation

The problem of attribution represents the main obstacle, as it is technically difficult to determine whether an attack originates from a state or from non-state actors (Al-Obaidi, op cit , p. 77.)

The rules of the International Law Commission (ILC) stipulate that an act is attributable to the state if it is committed by its official organs or by persons acting under its direction or effective control (**Articles on Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission in 2001, p. 47**) , A practical example of this is the Nicaragua v. United States case International Court of Justice (ICJ), Case Concerning Military and Paramilitary Activities in and against Nicaragua (**Nicaragua v. United States of America**), **Merits, Judgment of 27 June 1986, ICJ Reports 1986, p. 106.**), which established the 'effective control' standard for attributing the acts of armed groups to states.

In this case (1986), the International Court of Justice ruled that mere indirect support is not sufficient to establish responsibility; rather, 'effective control' must be proven (**Schmitt, 2013, p 61**)

This is difficult to achieve in cyberattacks due to concealment and deception techniques. Consequently, cyberattacks cannot be attributed to a specific state unless there is strong evidence of its direct involvement or support.

A : International Mechanisms

The international community has recognized the seriousness of cyber threats, considering them no less dangerous than traditional military threats. Therefore, a number of legal and institutional frameworks have been established to address this phenomenon.

1. The United Nations

- The General Assembly

The General Assembly has issued guiding resolutions on the use of information and communication technologies in the context of international peace and security (such as Resolution 70/237 of 2015). It plays a central role in discussing cybersecurity issues, especially given the lack of international consensus within the Security Council on classifying certain cyberattacks as threats to international peace and security.

As a universal body comprising all member states, the General Assembly serves as a primary forum for developing codes of conduct in cyberspace, through the adoption of legally non-binding but politically and normatively significant resolutions. It also established:

- The Group of Governmental Experts (GGE), which issued important reports in 2013, 2015, and 2021 affirming the application of the UN Charter to cyberspace, and the responsibility of states to prevent the use of their territories for launching attacks against other states (**United Nations, 2015, P 07**)
- The Open-ended Working Group (OEWG), which works to formulate international codes of responsible conduct in cyberspace, based on the principles of the UN Charter, ensuring respect for state sovereignty and non-interference in internal affairs.
- Since 2019, the OEWG has held a series of meetings, emphasizing the need to strengthen trust, cooperation, and capacity building among states, as well as to respect international humanitarian law in cases where cyberspace is used during armed conflicts (**United Nations General Assembly, 2018, p. 2.**)

- The Security Council

Some cyberattacks are considered threats to international peace and security. The Security Council is the UN's principal organ responsible for maintaining international peace and security under Chapter VII of the UN Charter. With the growing severity of cyber threats, discussions have emerged on whether certain large-scale cyberattacks may constitute threats to peace and security, similar to traditional military acts or international terrorism.

If a cyberattack disrupts critical infrastructure such as power grids, communication systems, or nuclear facilities, threatening the stability of a state or an entire region, the Security Council has the authority to intervene by issuing binding resolutions, ranging from imposing sanctions on the responsible state to authorizing the use of force (**Charter of the United Nations, 1945, p. 45**)

The Security Council has already discussed cybersecurity in several sessions on contemporary threats, with some member states arguing that cyberattacks may, in certain circumstances, amount to 'aggression,' while others stressed the need to distinguish between criminal cyber activities and cyberattacks that may constitute threats to peace and security (**UN Security Council, 2021, p. 6.**)

- International Documents

• General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), which entered into force in May 2018, is one of the most prominent regional legal frameworks that has had a wide impact on cybersecurity and privacy protection at the global level. Designed by the European Union to unify data protection rules across member states, it ensures a high level of protection of individuals' fundamental rights, particularly the right to privacy (**European Union, 2016, p. 45**)

The GDPR is not limited to the European regional framework but extends globally through the principle of extraterritoriality, obliging any company or institution, whether within the EU or abroad, to comply with its provisions if it processes personal data of European citizens (**Kuner, 2020, p. 17.**)

It is also a crucial tool in countering cyber-attacks, requiring organizations to adopt strict technical and organizational security measures to protect data and mandating compulsory reporting of data breaches within 72 hours. This has strengthened the culture of transparency and accountability in data management (**Voigt and von dem Bussche., 2017, p. 92.**)

Cyber Attacks under International Law

Thanks to these features, the GDPR has become a global standard in data protection, prompting many countries outside the EU to enact similar legislation, such as Brazil's LGPD and California's CCPA, making it a reference framework in shaping global cyber policies.

• The Budapest Convention (2001)

The Budapest Convention is the first binding international treaty aimed at combating cybercrime by harmonizing national legislation and enhancing judicial cooperation between member states, particularly in areas such as extradition and information sharing (Council of Europe, 2001, P 03)

• Draft Articles on the Responsibility of States for Internationally

Wrongful Acts Adopted by the International Law Commission in 2001, this draft represents one of the most important reference frameworks for determining state responsibility for acts that violate international law, including cyber-attacks. It sets out general rules obligating states to bear international responsibility if they commit wrongful acts or cause harm to another state through cyberspace.

Key provisions include:

- **Attribution:** Cyber-attacks must have been carried out by state officials or groups acting under the direction or support of the state.
- **International violation:** Such as breaching another state's sovereignty, threatening international peace and security, or violating human rights obligations.
- **Subsequent obligations:** Ending the violation, ensuring non-repetition, and compensating for the damage caused.

Thus, this draft is an essential tool for holding states accountable for cyber-attacks, provided attribution and responsibility can be proven (International Law Commission (ILC, 2001, p. 47.)

2 : INTERPOL

The International Criminal Police Organization (INTERPOL) plays a central role in combating cybercrime, given its transnational nature and the difficulty of tracking perpetrators within national jurisdictions. In 2015, INTERPOL established the Global Complex for Innovation (IGCI) in Singapore as a platform for coordinating international efforts against cyber threats and providing technical

and training support to law enforcement agencies in member states (**INTERPOL, 2016, P 12**)

INTERPOL works on exchanging digital intelligence among member states, developing advanced tools for digital forensics, and coordinating joint operations to combat hacking networks and online fraud worldwide (**INTERPOL, 2019, P 08**)

It also organizes training programs and international conferences to build police capacity in areas such as digital evidence, attacks on critical infrastructure, and online financial crimes. In doing so, INTERPOL enhances international cooperation to counter cybercrimes that threaten global security and stability (**INTERPOL, 2020, P 27**)

B : Regional Mechanisms

1 : The European Union (EU)

In 2013, the EU adopted the European Cybersecurity Strategy, laying the foundation for strengthening member states' defensive capabilities against cyber threats through information sharing, developing national capacities, and establishing a Computer Emergency Response Team (CERT) (**European Union. Cybersecurity Strategy of the European Union, 2013, P 12**)

The European Union Agency for Cybersecurity (ENISA) plays a central role in supporting EU policies, building capacities, analyzing threats, and developing crisis response mechanisms (**ENISA, 2018, P 34**)

Additionally, the EU adopted the NIS Directive, the first comprehensive European legislation aimed at strengthening digital infrastructure security. It requires member states to establish national authorities and create mechanisms for cooperation and information exchange (**European Union, 2016, P 07**)

In 2020, the EU launched the Cybersecurity Strategy for the Digital Decade, aligning with rapid digital transformations. It focuses on enhancing cyber resilience of critical infrastructure, expanding public-private cooperation, and fostering innovation in areas such as AI and secure encryption, ensuring the protection of citizens' fundamental rights in cyberspace (**European Union, 2020, P 09**)

In this context, the European Union has undertaken several initiatives to strengthen cybersecurity. One example is the establishment of Computer Emergency Response Teams (CERT-EU) to address cyber-attacks against EU institutions (**Madeline, 2016, P 42**)

In addition, the Network and Information Security (NIS) Directive of 2016 required member states to create national authorities and enhance mechanisms for cooperation and information sharing (**Christou, 2018, P 77**)

The General Data Protection Regulation (GDPR) further linked data protection with cybersecurity by imposing strict compliance standards on organizations (**Kuner, 2020, P 105**), The European Union Agency for Cybersecurity (ENISA) also organizes Cyber Europe Exercises to simulate large-scale cyber incidents and assess preparedness (**Annegret, 2018, P 34**)

Moreover, the EU Cybersecurity Strategy 2020 focused on protecting critical infrastructure such as energy, transport, and healthcare systems (**European Commission. The EU's Cybersecurity Strategy for the Digital Decade. Brussels: European Commission, 2020, P 09**), Finally, the Union strengthened cooperation with the private sector by supporting innovation in artificial intelligence and secure encryption technologies (**Bradshaw, and Millard, 2021, pp. 50–65, P 52**)

2: The African Union (AU)

The AU has paid growing attention to cybersecurity and data protection. In 2014, it adopted the African Union Convention on Cybersecurity and Personal Data Protection (the Malabo Convention), the first regional legal framework aimed at establishing common rules for combating cybercrime, fostering digital trust, and safeguarding privacy (**African Union, 2014, P 12**)

The AU Commission also develops programs and policies to strengthen cooperation among member states against cyber threats through technical capacity building and information sharing. The AU collaborates with partners such as the EU and UN to improve digital infrastructure and protect critical systems from cyber-attacks (**African Union, 2018, P 22**)

These efforts help bridge legal and technical gaps between African states, laying the foundation for a regional approach complementary to international standards such as the GDPR and UN cyber norms. Thus, the AU seeks to integrate digital security into its peace and security architecture.

3 : The League of Arab States (LAS)

The LAS has increasingly prioritized cybersecurity in light of cross-border digital threats targeting critical infrastructure in Arab states. Since 2012, it has adopted the Arab Cybersecurity Strategy as a regional framework to coordinate

Cyber Attacks under International Law

member states' efforts against cybercrime, protect Arab cyberspace, and enhance security and technical cooperation **(League of Arab States, 2012, P 15)**

Through the Council of Arab Interior Ministers and the Arab ICT Organization, the LAS has developed mechanisms for information sharing, training programs, and specialized conferences to strengthen national capabilities against cyber-attacks. It has also promoted model Arab legislation on cybercrime to serve as a reference for national laws **(League of Arab States, 2014, P 09)**

These initiatives aim to build a unified Arab approach to cybersecurity, complementing other regional and international frameworks, and contributing to regional stability in an era of rapid digital transformation.

4 : The North Atlantic Treaty Organization (NATO)

Since the early 2000s, NATO has recognized cyber threats as an integral part of security challenges, especially after the 2007 cyber-attack on Estonia, which marked a turning point in its cybersecurity approach **(NATO, 2011, P 03)**

NATO adopted a Cyber Defense Policy aimed at protecting its networks and integrating the cyber domain into its collective defense system under Article 5 of the Washington Treaty. This means cyber-attacks may be treated as armed attacks warranting a collective response **(NATO, 2014, P 15)**

It has also established specialized centers, most notably the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, which develops strategic studies, trains experts, and organizes major cyber defense exercises such as "Locked Shields." NATO also prioritizes cooperation with the EU and partner states to enhance information sharing and defensive capabilities against cyber threats **(NATO, 2020, P 22)**

Through these efforts, NATO seeks to strengthen deterrence and defense in cyberspace, recognizing it as a domain of conflict as critical as land, sea, air, and outer space.

Conclusion

This study makes it clear that cyber attacks have become a fundamental challenge to the international legal system. Conflicts are no longer confined to land, sea, or air, but have extended into the digital domain, where the interests of states and non-state actors intersect.

Cyber Attacks under International Law

Despite international efforts to establish rules regulating this sphere, the absence of a binding international treaty on cybersecurity leaves a legal vacuum that complicates the process of deterring and holding actors accountable.

Nevertheless, public international law—particularly the rules of the UN Charter—demonstrates its adaptability to new threats, as principles such as the prohibition on the use of force, non-intervention, and state sovereignty can indeed be applied to cyberspace.

The evolution of digital attacks from mere acts of sabotage to tools of war and cross-border terrorism compels the international community to reconsider mechanisms of cooperation and strengthen the current legal framework through new treaties and customary norms. Balancing national security with the protection of human rights in cyberspace also remains a pressing challenge. From this analysis, we may conclude the following:

- **Applicability of traditional rules:** the fundamental principles of public international law, such as state sovereignty and the prohibition of intervention, can apply to cyberspace.
- **Absence of a binding international framework:** no comprehensive international treaty has yet been established to clearly regulate cyber attacks, leaving room for divergent interpretations.
- **State responsibility:** a state is legally responsible if it conducts, supports, or allows cyber attacks against another state.
- **The issue of legal classification:** debate continues over whether a cyber attack constitutes a “use of force” or an “armed attack” under the UN Charter.
- **The growing role of non-state actors:** terrorist groups and hackers now represent real threats that are no less dangerous than those posed by states.

Accordingly, the following recommendations are proposed:

- Conclude a specialized international convention on cybersecurity—similar to the Geneva Conventions—aimed at regulating the use of cyberspace in both peace and war.
- Strengthen international cooperation by establishing coordination mechanisms within the United Nations to monitor cyber attacks and enhance intelligence sharing between states.
- Develop attribution standards by setting precise technical and legal rules for identifying the source of cyber attacks, in order to prevent false accusations.
- Draft laws that protect against cybercrime while safeguarding freedom of expression and privacy.

Cyber Attacks under International Law

- Integrate cybersecurity into national policies through technical capacity-building, legal training, and strengthening domestic legislation.

Bibliography

Books

1. Michael N Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013
2. Thomas Rid., *Cyber War Will Not Take Place*. Oxford: Oxford University Press, 2013
3. European Union., *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels: European Commission, 2013
4. Oona A Hathaway and others., "The Law of Cyber-Attack", *California Law Review*, Vol. 100, 2012
5. Eneken Tikk., *International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO CCD COE Publications, 2017
6. Ahmed Al-Obaidi, *International Law and Cyberspace*, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2020.
7. Nicolas Falliere, Liam O. Murchu, and Eric Chien, "W32.Stuxnet Dossier," Symantec Security Response, Version 1.4 , 2011
8. Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," *Proceedings of the 7th European Conference on Information Warfare and Security* ,2008
9. Kuner Christopher., *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2020
10. Paul Voigt and Axel von dem Bussche., *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017
11. Carr Madeline. *US Power and the Internet in International Relations: The Irony of the Information Age*. London: Palgrave Macmillan, 2016
12. Christou George. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. London: Palgrave Macmillan, 2018,
13. Kuner Christopher. *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press, 2020
14. Bendiek, Annegret. *European Cybersecurity Policy*. Berlin: Stiftung Wissenschaft und Politik (SWP Research Paper), 2018
15. European Commission. *The EU's Cybersecurity Strategy for the Digital Decade*. Brussels: European Commission, 2020
16. Bradshaw, Simon, and Christopher Millard. *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*. *International Data Privacy Law*, Vol. 11, No. 2, 2021, pp. 50–65

International Documents

1. International Court of Justice (ICJ), *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment of 27 June 1986, ICJ Reports 1986
2. International Committee of the Red Cross (ICRC), *International Humanitarian Law and Cyber Operations during Armed Conflicts*, Geneva: ICRC, 2019
3. Council of Europe, *Convention on Cybercrime (Budapest Convention)*, Budapest, 23 November 2001. European Treaty Series – No. 185

Cyber Attacks under International Law

4. Articles on Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission in 2001, United Nations, Official Records of the General Assembly, Fifty-sixth session, Supplement No. 10 (A/56/10), 2001
5. United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015
6. United Nations General Assembly, “Advancing responsible State behaviour in cyberspace in the context of international security”, Resolution 73/27, A/RES/73/27, adopted on 5 December 2018
7. Charter of the United Nations, Article 39, UN, 1945
8. UN Security Council, “Cybersecurity and International Peace and Security”, Report of the Security Council, 2021
9. European Union, General Data Protection Regulation, Regulation (EU) 2016/679, 2016
10. Council of Europe, Budapest Convention, 2001
11. International Law Commission (ILC), Draft Articles on Responsibility of States for Internationally Wrongful Acts, United Nations, 2001
12. INTERPOL, Annual Report, 2016
13. INTERPOL, Cybercrime Strategy, 2019
14. INTERPOL, Annual Report, 2020
15. European Union. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels: European Commission, 7 February 2013
16. ENISA. Annual Report 2018. European Union Agency for Network and Information Security, 2018
17. European Union. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). Official Journal of the European Union, L 194, 19 July 2016
18. European Union. The EU's Cybersecurity Strategy for the Digital Decade. Brussels: European Commission, 16 December 2020
19. African Union, Convention on Cyber Security and Personal Data Protection, Malabo, 2014
20. African Union, Annual Report on Cybersecurity, 2018
21. League of Arab States, Arab Cybersecurity Strategy, 2012
22. League of Arab States, Model Arab Law on Cybercrime, 2014
23. NATO, Cyber Defence Policy, 2011
24. NATO, Wales Summit Declaration, 2014
25. NATO, Annual Cyber Defence Report, 2020