Workshop Summary Report

International Law and the Behaviour of States in the Use of ICT – Challenges and Opportunities

UNIDIR Security and Technology Programme

Acknowledgements

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. This report summarizes the discussions held during a workshop organized by UNIDIR's Security and Technology Programme with the generous support from the Governments of China, Czechia, France, Germany, the Netherlands, the Russian Federation, Switzerland and the United Kingdom.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

About the Author

This report was produced by the **UNIDIR's Security and Technology Programme**; Cecile Aptel, Samuele Dominioni, Andraz Kastelic, Moliehi Makumane and Giacomo Persi Paoli contributed to this report.

Table of Contents

+ 41 (0)22 917 1141 | **unidir.org** | **unidir@un.org** | Palais des Nations, CH-1211 Geneva 10 Switzerland

Executive Summary

The workshop "International Law and the Behaviour of States in the Use of ICT – Challenges and Opportunities", held in Geneva, 15 November 2023, facilitated a structured discussion among State representatives on the application of international legal principles of sovereignty and peaceful settlement of disputes in the context of State use of information and communication technologies (ICT). Sixty-two representatives and legal experts from 23 States participated at the event. This workshop was a first of its kind and served as pilot project. Based on the positive feedback received, UNIDIR plans to organize additional workshops of this kind involving a wider selection of Member States.

This report provides a summary of the substantive discussions, in particular on convergent and divergent relevant national positions and questions raised during the discussions. It is hoped that the report will assist Member States in their deliberations on ICT in the context international peace and security and, in particular, guide multilateral discussions on how international law applies to cyberspace.

The exchanges during the workshop indicated a number of convergent national views on how existing international law, particularly the prohibitions of the use of force and of intervention, and peaceful settlement of disputes, apply in cyberspace. At the same time, the workshop outcomes suggest that States continue to disagree on whether the existing international rules and expectations of State behaviour in cyberspace are indeed a sufficient framework for peace and stability in the ICT environment, or whether the particular character of ICT threats necessitates a new, dedicated international treaty.

+ 41 (0)22 917 1141 | **unidir.org** | **unidir@un.org** | Palais des Nations, CH-1211 Geneva 10 Switzerland

1 Introduction

This year marks quarter of a century since States expressed the concern that information and communication technologies (ICT) "can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States".[1] Ever since, States have been deliberating on the developments in the field of ICT in the context of international security and seeking an agreement under the auspices of the United Nations on international efforts to enhance international ICT security.

Upon the agreement of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security in 2013 that international law, and in particular the Charter of the United Nations, applies to the State use of ICT—an outcome that was welcomed by the General Assembly in the same year[2]—States continue to study how international law applies to State behaviour in the digital domain, including though exchange of relevant national statements and State practice.[3]

A persisting point of contention in this regard, observed as recently as the fifth session of the Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021–2025 in July 2023, is whether existing international law is sufficient to effectively govern the behaviour of States in the use of ICT. Some States argue that existing international law and voluntary norms provide a "robust and well-established framework to address the use of ICTs by States".[4] Some States, on the other hand, advocate for the codification of a new, dedicated legal regime to close the gaps in the existing international law.[5]

To facilitate an exchange of views, UNIDIR's Security & Technology Programme convened a closed-door expert workshop **involving 62 State representatives and legal experts from 23 States**[6] focused on substantive deliberation on international law and State use of ICT in the context of international security. The main purpose of the workshop was to explore the extent to which existing international law can, or cannot, prevent and settle potential inter-State conflicts by peaceful means and maintain international peace and security in the ICT

[1] General Assembly, A/RES/53/70, 4 January 1999.
[2] General Assembly, A/RES/68/243, 20 December 2013.
[3] General Assembly A/78/265, 1 August 2023.
[4] Australia, Colombia, El Salvador, Estonia, Uruguay, "Applicability of international law, in particular the United Nations Charter, in the use of ICTs: areas of convergence", OEWG Working Paper, 24 July 2023), <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Cyber_OEWG_-_International_Law_APR_paper_-_updated_-_24_July_2023.pdf>.
[5] Promoting the idea, and in response to the General Assembly resolutions 76/19 and 77/36 "noting the possibility of future elaboration of additional binding obligations, if appropriate", a number of States co-sponsored the "Concept of the Convention of the United Nations on Ensuring International Information Security", submitted to the seventy-seventh session of the General Assembly, as well as to the OEWG 2021–2025; see General Assembly A/78/265, 1 August 2023, Annex D.
[6] Australia, the Bolivarian Republic of Venezuela, Brazil, Canada, China, Colombia, Cuba, Czechia, Estonia, France, Germany, Islamic Republic of Iran, Italy, Japan, Kenya, Mexico, the Netherlands, Nicaragua, the Russian Federation, Singapore, Switzerland, the United Kingdom, and the United States.

+ 41 (0)22 917 1141 | **unidir.org** | **unidir@un.org** | Palais des Nations, CH-1211 Geneva 10 Switzerland

environment. To this end, the workshop provided a platform for sharing interpretations of how international law applies to State use of ICT in response to specific scenarios, and for discussing possible challenges related to its application and related solutions such as the elaboration of new norms, including legally binding ones.[7] As such, the workshop aimed to facilitate transparency and to promote confidence among States—confidence-building is an important aspect of multilateral discussion in the context of international law and State use of ICT[8] and the potential of confidence-building measures to "promote stability and help to reduce the risk of misunderstanding, escalation and conflict" is universally recognized.[9]

1.1 Methodology of the workshop

To facilitate substantive discussions, UNIDIR prepared a **set of scenarios describing fictional ICT incidents** involving two or more States, thus providing a context for deliberation on how international law might apply as well as the potential, associated challenges. The workshop scenarios guided the participants to consider **the international legal principles of sovereignty** (including the resulting obligation of non-intervention and the prohibitions of the threat or use of force) **and of peaceful settlement of disputes**, both explicitly confirmed by the General Assembly as applicable to State behaviour in the use of ICT.[10]

The workshop participants were invited to share views on the application of international law in the ICT domain and, in particular, to reflect on the following **guiding questions**:

a) How does existing international law apply in the given situation?
b) What measures of reaction are the States involved in the scenario permitted to pursue under existing international law?
c) What are the challenges or limitations with the application of existing international law?
d) How can these potential challenges be resolved? Among the possible solutions, to what extent could continued discussion and exchanges of views by States on how specific rules and principles of international law apply to the use of ICT by States, and potential development of new norms, if necessary, contribute to addressing such challenges?

This workshop was a first of its kind and served as pilot project. Based on the positive feedback received, UNIDIR plans to organize additional workshops of this kind involving a wider selection of Member States.

[7] General Assembly A/78/265, 1 August 2023, Annex, para. 32.
[8] See General Assembly A/77/275, 8 August 2022.
[9] General Assembly A/76/135, 14 July 2021, para. 74.
[10] See, e.g., General Assembly A/78/265, 1 August 2023.

+ 41 (0)22 917 1141 | **unidir.org** | **unidir@un.org** | Palais des Nations, CH-1211 Geneva 10 Switzerland

1.2 The scope and purpose of the report

This report provides a summary of the substantive discussions held at the workshop. Focusing on **convergent and divergent views** as well as some of the questions that remain to be explored, the report outlines venues of possible future multilateral discussions related to international law in cyberspace.

Readers are encouraged to study this report in conjunction with the **report of UNIDIR's Cyber Stability Conference 2023**,[11] which summarized the substantive discussions on the application of the law of the Charter of the United Nations in the context of the behaviour of States in their use of ICT, including the prohibition of the use of force and law of peaceful settlement of disputes.

2 Summary of the Substantive Discussions

Substantive workshop discussions primarily focused on the principles of **sovereignty** and **peaceful settlement of disputes**. Ad hoc discussions also considered a number of other legal considerations related to international **law of State responsibility** and the **principle of due diligence.** The discussions are summarized below.

2.1 Sovereignty

There was general agreement that the principle of sovereignty, a cardinal principle of contemporary international law,[12] applies to State use of ICT. This reflects the consensus reached in the context of the OEWG 2021–2025,[13] as well as a number of individual State positions and the Concept of the Convention of the United Nations on Ensuring International Information Security.[14]

2.1.1 Sovereignty as a rule of international law

During the workshop discussions, most of the participating States held that sovereignty is not only a principle but also a primary rule of international law[15] and that cyber operations indeed have the potential to violate it; a breach of the rule could result in international responsibility.

[11] Security & Technology Programme, "2023 Cyber Stability Conference Summary Report: Use of ICTs by States: Rights and Responsibilities Under the Charter of the United Nations", UNIDIR, 2023, <https://unidir.org/publication/use-of-icts-by-states-rights-and-responsibilities-under-the-un-charter/>.
[12] Sovereignty denotes State independence and is based on the exclusive power that it exercises over its territory and its nationals. Sovereignty can be exercised in relation to internal affairs (internal sovereignty) as well as external affairs (external sovereignty). While related, sovereignty is not to be conflated with sovereign equality, denoting equal rank of every State to other sovereign States; see Samantha Besson, "Sovereignty", Max Planck Encyclopedia of Public International Law, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1472>.
[13] General Assembly A/78/265, 1 August 2023, para. 30.
[14] Ibid, Annex D.
[15] "International legal rules represent the obligations of States, as found in sources of international law such as treaties, customary international law, general principles of law recognized by community of nations, judicial decisions, and the writings of the most prominent scholars. Principles of international law are more general

+ 41 (0)22 917 1141 | unidir.org | unidir@un.org | Palais des Nations, CH-1211 Geneva 10 Switzerland

For a majority of the participating States, an act of planting malware into or tampering with the integrity of a system under foreign jurisdiction would not likely be interpreted as a violation of sovereignty. That assessment could however change depending on the nature of the targeted system; some participants were of the opinion that planting malware into critical national infrastructure would run contra the obligation to respect sovereignty.

Most of the State representatives argued that sovereignty would likely be violated if a cyber operation resulted in a physical damage to a system;[16] legal assessment would be more challenging in the event of a malicious ICT incident altering or erasing the data of a system under sovereign jurisdiction. In this case, the assessment would likely depend on the scale of impact of the malicious ICT act.

2.1.2 Non-intervention

Participants generally appreciated the distinction between lawful interference[17] and unlawful intervention. In discussing the obligation of non-intervention,[18] participants reaffirmed the customary condition of coercion for interference to constitute intervention, prohibited under international law. A number of participants argued that coercion equals deprivation of a State's freedom of control over its *domaine réservé*.[19]

A clear connection between a cyber operation and its consequences, some suggested, is imperative in order to establish a violation of the obligation of non-intervention. Furthermore, when assessing the consequences of a cyber operation, one should consider all (reasonably) foreseeable and not only immediate effects.

In evaluating an ICT incident, and with a view of establishing whether it constituted a prohibited intervention, some States listed the following factors as imperative to consider:

---

pronouncements of the fundamental objectives of law. They lack technical precision, methods, or criteria related to the attainment of these objectives. Principles of international law can therefore serve a different purpose and may be useful for systematizing or interpreting legal rules. They do not automatically impose legal obligations, even if they give rise to specific legal obligations"; Andraz Kastelic, "Due Diligence in Cyberspace: Normative Expectations of Reciprocal Protection of International Legal Rights", UNIDIR, 2021.

[16] See *2.1.3 Prohibition of the threat or use of force* below.

[17] See n (18).

[18] "No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State"; General Assembly A/RES/2625(XXV), 24 October 1970. Intervention if distinct from interference. It is widely accepted that "the interference must be forcible or dictatorial, or otherwise coercive, in effect depriving the State intervened against of control over the matter in question. Interference pure and simple is not intervention"; Robert Jennings, Arthur Watts, eds., "Oppenheim's International Law", Vol. I, 9th ed., Oxford University Press 2008, 432; see also International Court of Justice, "Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)", Merits, Judgment, ICJ Reports 1986.

[19] The concept of *domaine réservé* is central to the principle of sovereignty: "it describes the areas of State activity that are internal or domestic affairs of a State and are therefore within its domestic jurisdiction or competence"; Katja S Ziegler, "Domaine reserve", Max Planck Encyclopedia of Public International Law, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1398?rskey=DDuXYD&result=1&prd=OPIL>.

+ 41 (0)22 917 1141 | **unidir.org** | **unidir@un.org** | Palais des Nations, CH-1211 Geneva 10 Switzerland

- the degree of impact on the ability of a State to exercise its sovereignty, including the temporal aspect of the impact;
- the nature of the target; and
- the objective of the malicious ICT operation or the intent of the perpetrator.

2.1.3 Prohibition of the threat or use of force

Generally, State representatives agreed that the threshold for a cyber operation to qualify as a prohibited use of force is rather high; some suggested only cyber operations with consequences equivalent to kinetic use of force should be labelled as forcible, thus in contravention to the prohibition under Article 2(4) of the Charter of the United Nations.

One of the fictional scenarios discussed by participants involved a cyber operation that led to physical damage of production facilities; there was a general agreement among participants that physical damage to an object caused by an ICT operation could indeed constitute use of force. The participants did not discuss the legal qualification of a cyber operation resulting in injury to human beings; outcomes of the previous dialogues facilitated by UNIDIR suggest possible convergence among States that ICT operations causing injury to human beings could be interpreted as use of force.[20]

Conversely, no consensus has been reached on the status of computer data. Despite some participants arguing that data is protected under the principle of sovereignty, States have not agreed on the qualification of a cyber operation that leads to the destruction of data.

2.2 Peaceful settlement of disputes

Much like the principle of sovereignty, the applicability of the law of peaceful settlement of disputes to disputes arising from State use of ICT proved to be unchallenged among the State representatives. This too is a reflection of the past international declarations.[21]

Throughout the discussions, State representatives recalled various forms of peaceful settlement of disputes recognized by the Charter of the United Nations[22] and underscored that the dispute settlement process can only start after all parties to the dispute have come to an agreement on the specific form of the settlement process. In other words, no State can be compelled to pursue a particular form of dispute settlement.

An important principle underlying the peaceful settlement of disputes is that of good faith,[23] which was repeatedly highlighted by the State representatives attending the workshop. The

[20] Security & Technology Programme, "2023 Cyber Stability Conference Summary Report: Use of ICTs by States: Rights and Responsibilities Under the Charter of the United Nations", UNIDIR, 2023, <https://unidir.org/publication/use-of-icts-by-states-rights-and-responsibilities-under-the-un-charter/>, 11.
[21] See, e.g., General Assembly A/78/265, 1 August 2023.
[22] Charter of the United Nations, 1945, 1 UNTS XVI, art. 33.
[23] General Assembly A/RES/2625(XXV), 24 October 1970.

+ 41 (0)22 917 1141 | **unidir.org** | **unidir@un.org** | Palais des Nations, CH-1211 Geneva 10 Switzerland

fact that States have an obligation to act in good faith when engaged in peaceful dispute resolution was not challenged by any of the State representatives.

In exploring the specific obligations of good faith, State representatives deliberated on the application of the duty of non-aggravation.[24] Accordingly, several participants held that any conduct frustrating or worsening the dispute at hand while engaged in a dispute settlement process would likely be seen as contra good faith and thus not permitted under existing international law. This is a reflection of the principle of good faith as established in international law.[25]

Some State representatives suggested that unauthorized intelligence gathering via ICT during a process of peaceful settlement of disputes would not be compliant with the good faith principle, while some suggested that any legal assessment of such conduct should take into consideration whether intelligence collection had negative impacts on the ability of a State to present a case in a given dispute settlement format before labelling it contra good faith.

In relation to this, a question on the legality of countermeasures[26] during the peaceful settlement of disputes was repeatedly raised. A number of State representatives argued that countermeasures, a lawful measure of self-help under the customary law of State responsibility,[27] could be in contravention of the good faith principle if taken during a peaceful dispute settlement process, particularly so if the disputed act had ceased. The legality of measures of retorsion[28] in the context of peaceful settlement of disputes arising from the State use of ICT, on the other hand, was not questioned by any of the participants.

Agreement emerged among the participants that further discussions are needed on countermeasures, in particular in the context of peaceful settlement of disputes.

[24] "States parties to an international dispute, as well as other states, shall refrain from any action whatsoever which may aggravate the situation so as to endanger the maintenance of international peace and security and make more difficult or impede the peaceful settlement of the dispute"; General Assembly A/RES/37/590, 15 November 1982, art. 8.
[25] See e.g. General Assembly A/RES/2625(XXV), 24 October 1970.
[26] Countermeasures denote non-punitive, compliance-inducing measures intended to secure cessation of and reparation for internationally wrongful conduct. Otherwise unlawful, wrongfulness of a countermeasure taken in response to an internationally wrongful act is precluded according to the customary international law of State responsibility; see General Assembly A/RES/56/83, 28 January 2002, annex.
[27] Ibid.
[28] Retorsion denote unfriendly measures of self-help taken by one State against another States, with the intention to induce compliance of the latter with its international obligations. Measures of retorsion "do not interfere with the target State's rights under international law" and are a well-established concept under the customary international law of State responsibility. Retorsion is to be distinguished from countermeasures; Thomas Giegerich, "Retorsion", Max Planck Encyclopedia of Public International Law, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e983>.

+ 41 (0)22 917 1141 | **unidir.org** | **unidir@un.org** | Palais des Nations, CH-1211 Geneva 10 Switzerland

2.3 Attribution and due diligence

2.3.1 Attribution

Inevitably, some of the positions expressed during the workshop touched upon the issue of attribution,[29] with some of the participants arguing that there is no established international law of evidence and thus no agreed evidentiary standards when considering attribution of unlawful cyber operations.

Not all participants agreed with this assessment, some arguing that States looking to establish legal attribution of a malicious ICT operation to a particular State should be able to present conclusive or compelling evidence. According to some, the standards of proof in relation to the attribution of an ICT operation to a State are not a matter of international law but a discretionary policy decision. State participants also disagreed during the course of discussions whether States are under an obligation to disclose evidence in support of attribution claims or is it merely an expectation of State behaviour as noted in the 2021 report of the Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,[30] subsequently welcomed by the General Assembly.[31] Indeed, as a matter of established customary international law, States have no obligation to discharge the burden of proof in extrajudicial settings.

Acknowledging technical challenges associated with attribution of ICT operations,[32] some participants warned of the consequences of erroneous attribution, which would render any countermeasures taken against a State not responsible for the ICT operation wrongful and could potentially lead to the escalation of conflict. To counter such challenges in attribution, some State representatives proposed the establishment of an impartial international attribution mechanism.

2.3.2 Due diligence

Ad hoc discussions also included the principle of due diligence,[33] widely recognized by participants as applicable to the fictional scenarios considered in the workshop. The relevant discussions focused on whether due diligence imposes legal obligations, namely of prevention

[29] There are three distinct if interrelated aspects of attribution: legal, technical and political. Legal attribution is guided by the customary law of State responsibility, and it denotes the ascription of a conduct of a natural person to a particular State; see Kastelic, Andraz. "Non-Escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics", UNIDIR, 2022.
[30] General Assembly A/76/135, 14 July 2021, para. 71(g).
[31] General Assembly A/RES/76/19, 8 December 2021.
[32] Andraz Kastelic, "Non-Escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics", UNIDIR, 2022.
[33] The due diligence principle of international law can be traced back to a seminal case of the International Court of Justice (ICJ), which argued in the Corfu Channel Case that a State is "not to allow knowingly its territory to be used for acts contrary to the rights of other States"; International Court of Justice, "Corfu Channel case", Merits, ICJ Reports 1949, <https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf>. See also Andraz Kastelic, "Due Diligence in Cyberspace: Normative Expectations of Reciprocal Protection of International Legal Rights", UNIDIR, 2021.

+ 41 (0)22 917 1141 | **unidir.org** | **unidir@un.org** | Palais des Nations, CH-1211 Geneva 10 Switzerland

and termination, or only prescribes voluntary expectations of State behaviour, as asserted by the 2021 GGE report, for instance.[34] The proponents of both interpretive approaches of due diligence in cyberspace recognized that States are only to act within the limits of their capacities.

3 Conclusion

The workshop "International Law and the Behaviour of States in the Use of ICTs – Challenges and Opportunities" facilitated a structured discussion among State representatives and legal experts on the application of international legal principles of sovereignty and the peaceful settlement of disputes in the context of State use of ICT. Despite the lack of consensus on whether existing international law and norms are a sufficient framework to ensure peace and stability in the ICT environment or whether a set of additional rules in the form of a new international treaty is needed, the substantive discussions on how international law applies to State use of ICT provided a number of conclusions:

- There was general agreement that the principle of sovereignty applies to State use of ICT.
- Most of the participants held that sovereignty is not only a principle but also a primary rule of international law; cyber operations have the potential to violate that rule.
- Although no agreement has been reached on the threshold of the violation of the rule of sovereignty, for the majority of participants, an act of planting malware into or tampering with the integrity of a system under foreign jurisdiction would not likely be interpreted as a violation of sovereignty unless that cyber operation resulted in physical damage to a system.
- Discussing the obligation of non-intervention, participants reaffirmed the customary condition of coercion for interference to constitute internationally unlawful intervention.
- A number of examples of coercive acts in cyberspace were discussed throughout the workshop; an act depriving a State's freedom of control over its *domaine réservé* was repeatedly suggested as coercive in the context of the ICT domain, although further clarity on the concept of coercion could enhance predictability of State behaviour in cyberspace and promote stability in the ICT domain.
- There was general agreement that ICT operations causing physical damage could constitute use of force. It remained to be resolved whether the destruction of computer data would also constitute a prohibited use of force.
- State representatives agreed that the law of peaceful settlement of disputes applies to disputes arising from State use of ICT. No State can be compelled to engage in a particular form of dispute settlement.
- State representatives agreed that the good faith principle is central to the peaceful settlement of disputes. The duty of non-aggravation was repeatedly invoked as the most important good faith obligation in the context of the peaceful settlement disputes. Other relevant good faith obligations, such as the obligations to preserve

[34] See General Assembly A/76/135, 14 July 2021, norm 13 (c).

+ 41 (0)22 917 1141 | **unidir.org** | **unidir@un.org** | Palais des Nations, CH-1211 Geneva 10 Switzerland

confidentiality or to protect legitimate expectations, did not receive due attention in discussions.

- Ad hoc discussions considered the law of State responsibility, including attribution and relevant evidentiary considerations, and the principle of due diligence. Remaining relevant questions include whether States must or should substantiate attribution claims, what are the legal standards of proof and which, if any, due diligence obligations extend to State conduct in cyberspace.

4 References

1. Australia, Colombia, El Salvador, Estonia, Uruguay, "Applicability of international law, in particular the United Nations Charter, in the use of ICTs: areas of convergence", OEWG Working Paper, 24 July 2023), <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Cyber_OEWG_-_International_Law_APR_paper_-_updated_-_24_July_2023.pdf>.
2. Besson, Samantha. "Sovereignty", Max Planck Encyclopedia of Public International Law, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1472>.
3. Charter of the United Nations, 1945, 1 UNTS XVI.
4. General Assembly A/RES/2625(XXV), 24 October 1970.
5. ---, A/RES/37/590, 15 November 1982.
6. ---, A/RES/53/70, 4 January 1999.
7. ---, A/RES/56/83, 28 January 2002, Annex.
8. ---, A/RES/68/243, 20 December 2013.
9. ---, A/76/135, 14 July 2021.
10. ---, A/RES/76/19, 8 December 2021.
11. ---, A/77/275, 8 August 2022.
12. ---, A/78/265, 1 August 2023.
13. Giegerich, Thomas. "Retorsion", Max Planck Encyclopedia of Public International Law, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e983>.
14. International Court of Justice, "Corfu Channel case", Merits, ICJ Reports 1949, <https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf>.
15. ---, "Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)", Merits, Judgment, ICJ Reports 1986.
16. Jennings, Robert, Arthur Watts, eds., "Oppenheim's International Law", Vol. I, 9th ed., Oxford University Press 2008.
17. Kastelic, Andraz. "Due Diligence in Cyberspace: Normative Expectations of Reciprocal Protection of International Legal Rights", UNIDIR, 2021.
18. Kastelic, Andraz. "Non-Escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics", UNIDIR, 2022.
19. Russian Federation, "Concept of the Convention of the United Nations on Ensuring International Information Security", OEWG Working Paper, 29 June 2023, <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_convention_on_ensuring_international_information_security.pdf>.
20. Security & Technology Programme, "2023 Cyber Stability Conference Summary Report: Use of ICTs by States: Rights and Responsibilities Under the Charter of the United Nations", UNIDIR, 2023, <https://unidir.org/publication/use-of-icts-by-states-rights-and-responsibilities-under-the-un-charter/>.
21. Ziegler, Katja S. "Domaine reserve", Max Planck Encyclopedia of Public International Law, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1398?rskey=DDuXYD&result=1&prd=OPIL>.

+ 41 (0)22 917 1141 | **unidir.org** | **unidir@un.org** | Palais des Nations, CH-1211 Geneva 10 Switzerland