



UNIDIR

CHARTER OF THE UNITED NATIONS
AND
STATUTE OF THE
INTERNATIONAL COURT OF JUSTICE



SAN FRANCISCO · 1945

CONFERENCE REPORT

2023 Cyber Stability Conference Summary Report

Use of ICTs by States: Rights and Responsibilities Under the Charter of the United Nations

UNIDIR SECURITY AND TECHNOLOGY PROGRAMME

Acknowledgements

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. This study was produced by the Security and Technology Programme, which is funded by the Governments of Czechia, Germany, Italy, the Netherlands, Norway and Switzerland, and by Microsoft. Andraz Kastelic, Lenka Filipova, Molihi Makumane and Samuele Dominioni contributed to this report.

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 necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

About the Author

This report was produced by **UNIDIR Security and Technology Programme**.

Contents

Executive Summary	5
1. INTRODUCTION	6
<hr/>	
1.1 Purpose of the Conference	7
1.2 Content of the Conference	7
1.3 Purpose of this summary report	8
2. SUMMARY OF THE CONFERENCE DISCUSSIONS	9
<hr/>	
2.1 Conference opening	9
2.2 Panel 1. Use of Armed Force and State use of ICTs	10
2.2.1 Can cyber operations violate the prohibition of the use of force?	11
2.2.2 When do cyber operations qualify as use of force?	11
2.2.3 When do cyber operations amount to the prohibited threat of force?	11
2.2.4 What lawful reactions are available to States targeted by cyber operations amounting to the use of force?	12
2.2.5 How does the Charter prohibition relate to cyber operations conducted by non-State actors?	13
2.3 Panel 2. Armed Attack and Self-Defence in Cyberspace	14
2.3.1 Does the law of self-defence apply in relation to ICT conduct?	15
2.3.2 Is there a difference between the use of force and an armed attack in the context of ICT operations and, if so, what is the threshold?	15
2.3.3 What are the legal limitations to taking measures of self-defence?	16
2.3.4 Can States resort to anticipatory or pre-emptive measures of self-defence?	16
2.4 Panel 3. Role and Powers of the Security Council	17
2.4.1 What is the role of the Security Council in respect to international ICT peace and security?	18
2.4.2 When does a cyber operation constitute a threat to or breach of peace?	18
2.4.3 When could a cyber operation constitute an aggression?	19
2.4.4 How can the Security Council ensure maintenance of international ICT peace and security?	19

2.5	Panel 4. Peaceful Settlement of Disputes	21
2.5.1	On the modalities of the peaceful settlement of disputes stemming from the State use of ICTs	22
2.5.2	How to facilitate peaceful settlement of disputes?	23
2.5.3	Should the international community aim to establish a dedicated peaceful settlement of disputes mechanism?	23
2.5.4	What is the role of the principle of good faith in peaceful settlement of disputes?	24
3. CONCLUSION AND SUGGESTIONS FOR THE FUTURE		25
<hr/>		
4. REFERENCES		27
<hr/>		

Executive Summary

The Cyber Stability Conference 2023 provided a platform for a substantive discussion on the application of the law of the Charter of the United Nations in the context of State conduct using information and communications technologies (ICTs). Specifically, the Conference deliberated on four areas of the law—use of force, armed attack and self-defence, role and powers of the Security Council, and peaceful settlement of disputes—with panellists, State representatives, focusing in their interventions on national interpretations of the law and State practice.

The purpose of the Conference was twofold: first, to advance the international discussions on how international law applies to cyberspace and to contribute to confidence-building by promoting transparency in order to reduce misperception and misunderstanding among the Member States and, second, to contribute to capacity-building by providing a platform for expert briefings and exchange of good practices.

This report provides a summary of the Conference briefings and discussions, an outline of the emerging convergent and divergent positions, as well as several suggestions for how to advance multilateral discussions on the application of international law to State conduct using ICTs and to ensure rule of international law in the twenty-first century. As such, the report charts the potential focus areas for future multilateral deliberations on the Charter and the use of ICTs in the context of international peace and security.





1. Introduction

As part of the mandate received by the General Assembly in 2013, the 4th Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security was tasked to study “how international law applies to the use of information and communications technologies by States”.¹ Ever since, relevant multilateral discussions have deliberated on the applicability of international law in cyberspace. International law is therefore a focus area also for the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 (OEWG 2021–2025).²

Despite the divergent national views on the appropriate normative regime in the context of State use of information and communications technologies (ICTs),³ almost a decade ago States agreed that existing international law, in particular the Charter of the United Nations, applies to cyberspace.⁴ Per the recommendation of the OEWG 2021–2025, to facilitate predictability of behaviour in cyberspace and to promote international peace and security, States should continue discussing how international law applies.⁵ The increasing frequency, sophistication and complexity of cyber threats⁶ further underline the urgency of these discussions.

1 General Assembly, A/RES/68/243, 9 January 2014.

2 General Assembly, A/RES/75/240, 4 January 2021.

3 See e.g. Russian Federation, “Updated Concept of the Convention of the United Nations on Ensuring International Information Security”, 29 June 2023, cosponsors Belarus and Nicaragua (unofficial translation), [https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-__\(2021\)/ENG_Concept_of_UN_Convention_on_International_Information_Security_Proposal_of_the_Russian_Federation_0.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-__(2021)/ENG_Concept_of_UN_Convention_on_International_Information_Security_Proposal_of_the_Russian_Federation_0.pdf).

4 General Assembly, A/RES/A/68/98, 24 June 2013; General Assembly, A/RES/68/243, 9 January 2014.

5 General Assembly, A/77/275, 8 August 2022, para. 6.

6 General Assembly, A/AC.290/2021/CRP.2, 10 March 2021.

1.1 Purpose of the Conference

Devised as a confidence- and capacity-building activity, the Cyber Stability Conference 2023 (CS23) organized by the United Nations Institute for Disarmament Research (UNIDIR) aimed to facilitate and complement the ongoing multilateral dialogue on the intricacies of the applicability of international law in the ICT domain.⁷

As a confidence-building activity, CS23 provided a platform for sharing national interpretations of international law in cyberspace and therefore aimed to reduce the uncertainties and mistrust among the States. Through exchange of practices and interpretations, **confidence-building** measures can enhance transparency and thus contribute to predictability and stability in international relations.

In addition to the exchange of views among the various national experts during CS23, substantive panels were preceded by introductory briefings from scholars. Both briefings as well as exchanges between national representatives aimed to contribute to **capacity-building** on matters of international law in cyberspace. Capacity-building in the context of international law in cyberspace supports the stability of the ICT domain by way of promotion of the rule of law, lawful use of ICTs and informed participation by all States in the relevant multilateral discussions.

1.2 Content of the Conference

To facilitate focused deliberations and therefore meaningfully contribute to the advancement of multilateral discussions, CS23 focused on the first source of international law that States agreed on as being applicable in cyberspace—the **Charter of the United Nations**.⁸

Based on this premise, CS23 explored the content and scope of legal principles, rights and obligations in cyberspace contained by the following applicable provisions of the Charter:

- prohibition of the use of armed force;
- armed attack and self-defence;
- role and powers of the Security Council; and
- peaceful settlement of disputes.

⁷ See General Assembly, A/77/275, 8 August 2022.

⁸ Ibid., annex, para. 15(a): “International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.”

1.3 Purpose of this summary report

The following is a summary of the substantive discussions on the application of the Charter in the context of State use of ICT in international relations. As such, the readers will benefit from an overview of convergent interpretations of the law as well as divergent positions as expressed by a number of Member States. Therefore, **this report indicates possible directions for the focused discussions of the future multilateral deliberations on ICTs in the context of international peace and security.**

To revisit the Conference in its entirety, please consult the video recording and other relevant resources available on the [dedicated conference webpage](#).





2. Summary of the Conference Discussions

2.1 Conference opening

In his opening address, **Robin Geiss**, Director of UNIDIR, emphasized the growing threat of malicious cyber operations, their potential to impact international peace and security and the need to advance multilateral deliberations on the substantive issues of the applicability of international law in the ICT domain.

The remarks of Director Geiss were followed by the address of **Izumi Nakamitsu**, United Nations Under-Secretary-General and High Representative for Disarmament Affairs. High Representative Nakamitsu emphasized the importance of the need to elaborate the responsibilities of States under the Charter in relation to cyberspace—a task, in her view, particularly urgent in the context of heightened malicious cyber activity in connection with the armed conflict in Ukraine.

The third opening address was delivered by Ambassador **Burhan Gafoor**, Permanent Representative of Singapore to the United Nations in New York and Chair of the OEWG 2021–2025. Ambassador Gafoor welcomed the timely nature of the conference discussions and the complementary nature of the Conference with the OEWG process. Additionally, Ambassador Gafoor emphasized the importance of the inclusive and democratic deliberations under the auspices of the United Nations on matters of international law in the ICT domain, which promote awareness, reduce capacity inequality and contribute to confidence-building among Member States.

2.2 Panel 1.

Use of Armed Force and State use of ICTs

The first panel discussed the concept of the use of force in the context of the ICT domain and lawful reactions by the injured State(s). The cardinal prohibition of the use of force, enshrined in article 2(4) of the Charter, is the cornerstone of international peace and security.

The initial expert briefing was provided by **Vera Rusinova**, Professor and Head of the School of International Law, National Research University Higher School of Economics, Russian Federation. Professor Rusinova outlined the traditional doctrine of the prohibition of the use of force, provided an overview of the doctrine in the context of ICT operations as interpreted by States and contemporary scholarship, and offered potential actions that States could take in seeking convergence on how the prohibition applies in the ICT domain.

The panel, moderated by **Giacomo Persi Paoli** of UNIDIR, featured the following discussants, elaborating national positions on the applicability of the prohibition of the use of force in the context of the ICT domain:

- **Marja Lehto**, Ambassador and Senior Expert, Ministry for Foreign Affairs, Finland;
- **Azucena Mayela Sahagún Segoviano**, Head of the Multilateral Treaties Department, Office of the Legal Adviser, Ministry of Foreign Affairs, Mexico; and
- **Robert M. Young**, Legal Counsel, Criminal, Security and Diplomatic Law Division, Global Affairs Canada.



2.2.1 Can cyber operations violate the prohibition of the use of force?

There was agreement among the speakers that the prohibition of the use of force is not limited to kinetic weapons. Indeed, and as argued by the International Court of Justice, Charter provisions prohibiting the use of force “do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed”.⁹ Accordingly, whether an act can be characterized as use of force or not depends not on the instrument used but on the effects of the act itself; cyber operations can thus potentially qualify as use of force.

2.2.2 When do cyber operations qualify as use of force?

All panellists addressed the question of the threshold of use of force and were in agreement that cyber operations causing physical damage or injury to human beings could indeed be interpreted as use of force. However, a number of speakers noted that every cyber operation needs to be assessed in the context of particular circumstances and should take into account indirect effects. Some speakers also cautioned that any detrimental effects of a cyber operation must be serious or significant in order to qualify as use of force.

What is less clear in relation to the threshold of use of force is whether the use of ICTs resulting in the disruption of critical services without physical effects or causing significant negative economic effect could be interpreted as use of force.

2.2.3 When do cyber operations amount to the prohibited threat of force?

Article 2(4) of the Charter not only prohibits use of force but also the threat of force. This has been acknowledged and deemed relevant also in the context of cyber operations during the first panel of CS23.

Some panellists argued that threat of force by means of ICTs becomes unlawful when the threat is sufficiently precise and directed against a State. In this context, the national interpretation of international law in cyberspace by Japan was given as an example by one of the speakers; according to the position, any cyber operation indicating “[State] intention or attitude of using force [...] unless its arguments or demands are accepted”¹⁰ constitutes a prohibited threat of force. Such interpretations closely follow the traditional understanding of article 2(4),¹¹ according to which mere possession of (cyber)weapons would not constitute threat of force.¹²

9 International Court of Justice, “Legality of the Threat or Use of Nuclear Weapons”, Advisory Opinion, ICJ Reports 1996, para. 39.

10 General Assembly, A/76/136, 13 July 2021, p. 49.

11 Ian Brownlie, “International Law and the Use of Force by States” (Oxford, Clarendon Oxford 1963) 364–5: “A threat of force consists in an express or implied promise by a government of a resort to force conditional on non-acceptance of certain demands of that government. If the promise is to resort to force in condition in which no justification for the use of force exists, the threat itself is illegal.”

12 For example, International Court of Justice, “Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)”, Merits, Judgment, ICJ Reports 1986, para. 269.

2.2.4 What lawful reactions are available to States targeted by cyber operations amounting to the use of force?

The panel speakers emphasized two instruments recognized as available to States targeted by a cyber operation amounting to the use of force—retorsion and countermeasures.

Retorsion consists of unfriendly reaction consistent with international obligations, short of the deprivation of the targeted State of its legal rights. Retorsion can take the form of, for instance, “the prohibition of or limitations upon normal diplomatic relations or other contacts, embargoes of various kinds or withdrawal of voluntary aid programmes”.¹³ According to the panellists, retorsion enables the injured State to signal unacceptable behaviour of States in cyberspace. Measures of retorsion can be taken also in response to the State behaviour that is inconsistent with the voluntary norms of responsible State behaviour in cyberspace.

Countermeasures on the other hand represent a legal category of reactions that consists of the deprivation of the responsible State of its legal rights. When taken in accordance with the conditions of the customary law of State responsibility, countermeasures are precluded from wrongfulness. “Countermeasures are a feature of a decentralized system by which injured States may seek to vindicate their rights and to restore the legal relationship with the responsible State which has been ruptured by the internationally wrongful act”,¹⁴ which includes use of force by ICT means. According to the panellists, the law of countermeasures is applicable to State use of ICTs and injured States can take countermeasures in response to the unlawful use of force by ICT means.



13 International Law Commission, “Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries”, Yearbook of the International Law Commission, 2001, vol. II, Part Two, p. 128.

14 Ibid.

2.2.5 How does the Charter prohibition relate to cyber operations conducted by non-State actors?

Reflecting the sentiment of the OEWG 2021 consensus report, the first panel expressed concern over growing numbers of ICT incidents involving non-State actors, some of which “demonstrated ICT capabilities previously only available to States”.¹⁵

The prohibition of the use of force, however, only applies to the conduct of States. The conduct of non-State actors involves responsibility of States only when there is a clear legal nexus between the two. The conditions of establishing the legal nexus are prescribed by the customary law of attribution.¹⁶ Some of the panellists also emphasized the responsibility of States for the lack of diligence in respect to the cyber conduct of non-State actors that amounts to the use of force. Indeed, as per the norm C of the Group of Governmental Experts 2021 report, States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.¹⁷

Given the non-binding and voluntary nature of the norms, failing to exhibit diligence results in political, and not legal, responsibility, which limits the lawful reaction to retorsion. Note, however, that some States have taken the position that norm C is a reflection of customary international law and States must not allow their territories to be used for internationally wrongful acts.¹⁸



15 General Assembly, A/AC.290/2021/CRP.2, 10 March 2021, para. 16.

16 International Law Commission, “Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries”, Yearbook of the International Law Commission, 2001, vol. II, Part Two; see also Andraz Kastelic, “Due diligence in cyberspace: Normative expectations of reciprocal protection of international legal rights”, UNIDIR, 2021.

17 General Assembly, A/76/135, 14 July 2021, norm 13(c).

18 See Andraz Kastelic, “Due diligence in cyberspace: Normative expectations of reciprocal protection of international legal rights”, UNIDIR, 2021.

2.3 Panel 2.

Armed Attack and Self-Defence in Cyberspace

This panel discussed the concept of an armed attack in cyberspace and self-defence. Self-defence is one of the two permitted derogations from the prohibition of the use of force, discussed in the preceding panel. It is a customary right,¹⁹ codified in article 51 of the Charter.

The initial expert briefing was provided by **Andraz Kastelic** of UNIDIR, outlining the traditional understanding of the doctrine and existing interpretations of the law in the context of State use of ICTs. Specifically, the initial briefing provided the audience with an introduction to the concept of an armed attack being distinct from the use of force, to the normative limitations to the right to self-defence, to applicable legal principles (necessity and proportionality) and to procedural requirements of taking measures in self-defence. The briefing concluded with an overview of the existing national interpretations of the law in the cyber domain.

The panel, moderated by **Katherine Prizeman** of the Office for Disarmament Affairs, featured the following discussants, elaborating national positions on the applicability of the law of armed attack and self-defence:

- **Artur R. Lyukmanov**, Director, Foreign Ministry's Department of International Information Security, Russian Federation;
- **John Reyels**, Head, Cyber Policy Coordination Staff, Federal Foreign Office, Germany;
- **Maitê de Souza Schmitz**, Counsellor, Ministry of Foreign Affairs, Brazil; and
- **Briony Daley Whitworth**, Director, Cyber Affairs and Critical Technology Branch, Department of Foreign Affairs and Trade, Australia.



¹⁹ International Court of Justice, “Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)”, Merits, Judgment, ICJ Reports 1986.

2.3.1 Does the law of self-defence apply in relation to ICT conduct?

A majority of the panellists reiterated the agreement of the 2022 Annual Progress Report of the OEWG, in which States also recalled and reaffirmed previous relevant consensus multilateral outcomes, namely that “international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment”.²⁰ One of the speakers expressed strong reservations about the applicability of the law of self-defence in the context of the cyber domain, while another cautioned about the conceptual differences between kinetic means and ICT means, which would warrant caution in further relevant substantive discussions.

Specifically, a point of divergence remains the disagreement on whether cyber operations can constitute an armed attack and whether self-defence is permitted in response to an ICT operation. One of the speakers argued that ICTs cannot be considered a weapon and urged the international community to continue deliberating on the topic at hand and to consider negotiating a new convention establishing a dedicated legal regime governing ICT threats to international peace and security.

Two speakers however rejected that proposition and argued that a cyber operation can indeed be considered an armed attack when the consequences are akin to those caused by a kinetic weapon. As illustrated by one of the panellists, an attack against a purification water plant causing human casualties, for example, could be considered an armed attack.

2.3.2 Is there a difference between the use of force and an armed attack in the context of ICT operations and, if so, what is the threshold?

According to article 51 of the Charter, the right to self-defence is conditioned by the occurrence of an armed attack.²¹ International jurisprudence suggests that armed attack is distinct from the use of force and not every use of force gives rise to the right to self-defence. The traditional doctrinal delineation between the two legal categories is based on the assessment of the “scale and effects”²² of the conduct in question, with only the “most grave”²³ occurrences of the use of force reaching the threshold of an armed attack, giving right to self-defence.

This distinction has been adopted in the context of cyber operations by a majority of the speakers of the second panel, with one specifically pointing to the need for assessing all foreseeable effects of a cyber operations in order to determine the gravity of a cyber operation. A number of hypothetical scenarios where States reserve the right to self-defence were presented; most frequently these scenarios involved examples of cyber operations targeting critical infrastructure assets. A particular issue in need of further analysis, argued one speaker, are cyber operations which do not cause any physical effects but may still be considered grave enough to constitute armed attack, giving rise to self-defence.

20 General Assembly, A/AC.292/2022/CRP.1, 28 July 2022, para. 2, referencing General Assembly, A/75/816, 18 March 2021, annex I, para. 7.

21 Nothing in the present Charter shall impair the inherent right of individual or collective self-defence *if an armed attack occurs* against a Member of the United Nations” [emphasis added]; Charter of the United Nations, 1945, 1 UNTS XVI, art. 51.

22 International Court of Justice, “Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)”, Merits, Judgment, ICJ Reports 1986, para. 195.

23 Ibid.

2.3.3 What are the legal limitations to taking measures of self-defence?

Self-defence is limited by well-established principles of international law—of necessity and of proportionality²⁴—which, argued one of the panellists, should always be considered. According to the principle of necessity, self-defence is only lawful if repelling an attack and preventing its success²⁵ could not have been achieved “without resort to force and that the degree of force employed did not exceed what was reasonably required for that purpose”.²⁶ The proportionality requirement, on the other hand, is satisfied when self-defence is proportional to “the threat posed by the armed attack”.²⁷ The panel also discussed lawful means of self-defence in reaction to a cyber operation amounting to an armed attack. Two of the panellists argued the law does not prescribe the means of self-defence and is thus permissive towards using conventional weapons in response to armed attack using ICTs. One of the speakers, nevertheless, urged caution and argued that considering kinetic response to armed cyber attack can be very dangerous.

The third consideration in respect to the limitations of self-defence heard during the panel was one related to procedure. This is prescribed by article 51 of the Charter, dictating that measures taken in exercise of the right are to be immediately reported to the Security Council.²⁸ One of the panellists emphasized the applicability of this procedural element of self-defence in the context of State use of ICTs.

2.3.4 Can States resort to anticipatory or pre-emptive measures of self-defence?

Although article 51 of the Charter permits States to take measures in self-defence only “if an armed attack occurs”,²⁹ legal theory and State practice suggests the possibility of self-defence before the occurrence of an armed attack and distinguishes between anticipatory and pre-emptive self-defence.³⁰ The distinction is also reflected in some of the national positions on the applicability of international law in relation to State use of ICTs.³¹ Two of the speakers on the second panel presented arguments in favour of anticipatory self-defence and thus the right to respond forcibly to a cyber attack considered as an armed attack and one that is reasonably established to be imminent.

24 See, e.g., International Court of Justice, “Oil Platforms (Islamic Republic of Iran v. United States of America)”, Judgment, ICJ Reports 2003, para. 51.

25 Roberto Ago, “Addendum - Eighth report on State responsibility by Mr. Roberto Ago, Special Rapporteur - the internationally wrongful act of the State, source of international responsibility (part 1)”, Yearbook of the International Law Commission, 1980, vol. II, Part One, para. 119.

26 Christopher Greenwood, “Self-Defence”, in Max Planck Encyclopedia of Public International Law (Oxford, Oxford University Press 2011), para. 27, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e401?rskey=dtukfv&result=1&prd=OPIL>.

27 Ibid., para. 28.

28 Charter of the United Nations, 1945, 1 UNTS XVI, art. 51.

29 Ibid.

30 Niaz A. Shah, “Self-defence, Anticipatory Self-defence and Pre-emption: International Law’s Response to Terrorism”, Journal of Conflict & Security Law, Spring 2007, vol. 12, no. 1 (Spring 2007), pp. 95–126.

31 See, e.g., France, “International Law Applied to Operations in Cyberspace: Paper shared by France with the Open-ended working group established by resolution 75/240”, 1 December 2021, p. 7, <https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf>.

2.4 Panel 3.

Role and Powers of the Security Council

The discussion of the third panel scrutinized chapters V and VII of the Charter in the context of State use of the ICTs. Specifically, the panel discussed the role and powers of the Security Council in respect to threats to and breaches of international peace and acts of aggression.

The initial expert briefing was provided by **Zhixiong Huang**, Professor and Vice Dean of the Law School, Wuhan University, China. Professor Huang introduced the law, including the role and powers of the Security Council, and provided an overview of the relevant outcomes of the ongoing and past multilateral discussions as well as a summary of national interpretations of the relevant provisions of the Charter.

The panel, moderated by **Andraz Kastelic** of UNIDIR, featured the following discussants:

- **Sheila Flynn**, Office Director, Global Policy, Plans, and Negotiations, International Cyberspace Security, Bureau of Cyberspace and Digital Policy, Department of State, United States;
- **Nathalie Jaarsma**, Ambassador at-Large for Security Policy and Cyber, Kingdom of the Netherlands; and
- **Tshenolo Sebusang**, Principal State Counsel, Ministry of Communications, Knowledge and Technology, Botswana.



2.4.1 What is the role of the Security Council in respect to international ICT peace and security?

The primary responsibility of the Security Council is “maintenance of international peace and security”,³² which remains relevant in the context of the ICT domain and has not been contested during CS23. According to two of the panellists, the fact that the Security Council has already engaged in the discussions on the matters of international ICT security indicates that cyber activities indeed have the potential to undermine international peace and security.

2.4.2 When does a cyber operation constitute a threat to or breach of peace?

According to the Charter, the Security Council may deliberate and act on a threat to peace, breach of peace or acts of aggression.³³ According to some of the panellists, only the most serious or destructive cyber incidents could be considered by the Security Council. For instance, a severe disruption of infrastructure through cyber means that would undermine international order would likely warrant the attention of the Security Council.

As argued by some during the panel, a cyber operation could qualify as a threat to peace and thus warrant deliberation by the Security Council if it caused instability on a large scale, even in the absence of force. This is different to a breach of peace, which is conditioned by the occurrence of the use of force; in establishing whether a cyber operation is ripe for consideration by the Security Council, the conduct could be evaluated based on its scale and effects.



32 Charter of the United Nations, 1945, 1 UNTS XVI, art. 24.

33 Ibid., art. 39.

2.4.3 When could a cyber operation constitute an aggression?

In addition to identifying threats to or breaches of peace, the Security Council may determine the existence of aggression, make recommendations or take measures in accordance with its mandate. In evaluating the situation and determining whether a situation has risen to the threshold of aggression, the Security Council is guided by the definition of aggression, annexed to the 1974 General Assembly resolution 3314 (XXIX),³⁴ which includes a list of examples of acts of aggression.³⁵

A number of panellists took note of that resolution and emphasized its continuous utility, including in the context of ICT operations. Arguments heard during the panel included that the definition is flexible enough to accommodate cyber operations, that the list of examples provided by the resolution is non-exhaustive, and that the definition of aggression could accommodate ICT operations in practice. A cyber operation causing irreversible damage to air fleet could be considered as an act of aggression, in an example given by one of the panellists.

2.4.4 How can the Security Council ensure maintenance of international ICT peace and security?

The oft-mentioned role of the Security Council in the context of international ICT peace and security is related to its indirect maintenance of international peace and security. Specifically, some of the panellists pointed out that the deliberative function of the Security Council can serve as a forum for discussion, be it in the form of Arria-formula meetings or periodic meetings. Indeed, in the recent past the Security Council has already availed itself of discussions in both formats related to the challenges of ICTs to international peace and security. These deliberation opportunities, complementing discussions in dedicated multilateral processes such as the OEWG, were welcomed by the panellists, recognizing their value for advancing common understanding of the norms of responsible State behaviour using ICTs, for building confidence among the States and for supporting capacity-building through sharing good practices.

To discharge its role, the Security Council can also “establish such subsidiary organs as it deems necessary”.³⁶ Such organs, as some conference panellists suggested, have an important role in investigating malicious cyber activities related to their given mandate. An example of a subsidiary organ which has previously utilized its investigative powers to consider the role of ICTs in the context of international peace and security is the Security Council Committee established pursuant to resolution 1718 (2006).³⁷

34 General Assembly, A/RES/3314(XXIX), 14 December 1974.

35 Ibid., art. 3.

36 Charter of the United Nations, 1945, 1 UNTS XVI, art. 29.

37 Security Council, S/RES/1718 (2006), 14 October 2006.

Sanctions, non-forcible measures authorized under the Charter article 41, are an important tool at the disposal of the Security Council for maintaining international peace and security. While some speakers recognized the value of these and the possibility of imposing sanctions by way of ICT means, they also warned that this is an underexplored mechanism in the context of cyber conduct and States should continue discussing the utility of such measures.

Moreover, the Security Council is empowered to establish peacekeeping forces. The panel discussed the potential of establishing peacekeeping forces dedicated to ensuring peace and security in the ICT domain. While the idea has not received any opposition, some panellists noted that it is only a subject of academic deliberation and States have not comprehensively discussed the potential of establishing such measures.



2.5 Panel 4. Peaceful Settlement of Disputes

This panel discussed the obligations imposed by the principle of peaceful settlement of disputes, potential venues of dispute settlement and the role of the principle of good faith.

The initial expert briefing was provided by **Hajer Gueldich**, Professor at the University of Carthage, Tunisia and Chairperson, African Union Commission on International Law. Professor Gueldich elaborated the traditional doctrinal understanding of the legal character of the principle of peaceful settlement of disputes and different means as recognized by law. The initial briefing provided conference participants with an integration of the principle in different regional legal instruments dedicated to cybersecurity and outlined national positions on the applicability of the principle of peaceful settlement of disputes and obligations of good faith.

The panel, moderated by **Moliehi Makumane** of UNIDIR, featured the following discussants:

- **Riccarda Chanda**, Deputy Permanent Representative, Permanent Mission to the United Nations, Switzerland;
- **Mohammad Aamir Khan**, Deputy Permanent Representative to the United Nations in New York, Pakistan; and
- **Harry Ormsby**, Legal Adviser, Foreign Commonwealth and Development Office, United Kingdom.



2.5.1 On the modalities of the peaceful settlement of disputes stemming from the State use of ICTs

Modalities of peaceful settlement of disputes are not prescribed by law. The Charter provides the following non-exhaustive list of modalities:

- negotiation;
- enquiry;
- mediation;
- conciliation;
- arbitration;
- judicial settlement;
- resort to regional agencies or arrangements; or
- other peaceful means, as chosen by the parties to the dispute.³⁸

Panellists agreed that States are free to choose a preferred modality in a given circumstance. However, a given modality is only a legitimate means for seeking peaceful settlement if it is accepted by all parties to the dispute.

Some of the speakers argued that peaceful settlement of disputes could be an effective mechanism for ensuring compliance with international law and should take precedence over measures of self-help, such as countermeasures.

A number of panellists also emphasized the importance of confidence-building measures (CBMs) to the peaceful settlement of disputes. It has been argued that CBMs could prevent misconceptions and even the emergence of tensions in relation to State conduct in the use of ICTs.

Not only do CBMs have the potential to prevent the emergence of a dispute but they can also facilitate the peaceful settlement of disputes that do arise. A specific example of such a CBM emphasized by the panellists was the Global Intergovernmental Points of Contact Directory,³⁹ currently under debate at the OEWG 2021–2025.⁴⁰

38 Charter of the United Nations, 1945, 1 UNTS XVI, art. 33.

39 Permanent Mission of Singapore to the United Nations New York, “Revised (Rev. 2) Paper on Draft Elements for the Development and Operationalization of a Global Intergovernmental Points of Contact Directory”, 8 May 2023, annex A, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/Chair's_Letter_8_May_2023_-_POC_directory.pdf.

40 Permanent Mission of Singapore to the United Nations New York, “Updated 2023 OEWG Meeting Schedule”, 6 April 2023, annex A, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/Letter_from_OEWG_Chair_6_April_2023.pdf.

2.5.2 How to facilitate peaceful settlement of disputes?

CBMs can promote transparency, and reduce misconceptions and tensions.⁴¹ According to the panellists, mistrust permeates international relations at the moment, which is why States could make use of various CBMs in order to reduce the likelihood of disputes in the first place.

Some speakers recognized the challenges resulting from a lack of an international agreement on how the law of peaceful settlement of disputes applies to State use of ICTs. According to one of the speakers, States could alleviate these challenges by sharing their national interpretation of the law and State practice and thus facilitate the peaceful settlement of disputes stemming from State use of ICTs.

One of the panellists also emphasized the role of the Secretary-General in promoting the peaceful settlement of disputes arising from ICT use. Examples of potential activities to be undertaken by the Secretary-General provided during the panel included active promotion of good offices⁴² and issuance of an annual report outlining the disputes resolved under the auspices of the United Nations, including ones alleging violations of international humanitarian law or fundamental principles of international law.

2.5.3 Should the international community aim to establish a dedicated peaceful settlement of disputes mechanism?

The question of a dedicated mechanism for the peaceful settlement of disputes arising from State use of ICTs proved to be divisive. Two of the panellists argued that States should make use of the existing mechanisms established by the Charter and, in order to facilitate this, should continue discussing the challenges that hinder the utility of existing mechanisms. In their view, it is imperative that States continue to share their interpretations of law in relation to cyberspace.

One of the speakers was of the opinion that the existing mechanisms are not appropriate for contemporary challenges and argued for the establishment of a peaceful settlement mechanism dedicated to settling disputes arising from State use of ICTs.

41 General Assembly, A/AC.290/2021/CRP.2, 10 March 2021, para. 41.

42 Office for Disarmament Affairs, "Securing Our Common Future: An Agenda for Disarmament", 2018, p. 56, <https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/06/sg-disarmament-agenda-pubs-page.pdf#view=Fit>.

2.5.4 What is the role of the principle of good faith in peaceful settlement of disputes?

The Charter prescribes compliance with the provisions in good faith.⁴³ The principle was recognized by all the panellists as applicable to State ICT conduct and relevant in the context of peaceful settlement of disputes. One speaker equated good faith with genuine intentions to settle the dispute.

Specific obligations under the principle, as suggested by one of the panellists, could include prohibition of misleading or lying, of undue delay and potentially of disclosure of evidence, particularly so when the party to a dispute is subject to a request to substantiate claims, such as the ones on attribution of malicious cyber operations.



⁴³ Charter of the United Nations, 1945, 1 UNTS XVI, art. 2(2).



3. Conclusion and suggestions for the future

CS23 provided a platform for discussion of the rights and obligations under the Charter in the context of State use of ICTs; in particular, the various panels discussed prohibition of the use of armed force, concepts of armed attack and self-defence, the role and powers of the Security Council in relation to ICT conduct, and peaceful settlement of disputes over ICT conduct.

A number of convergent views on how rights and obligations under the Charter apply in the context of State conduct in the ICT domain emerged. Namely, arguments that were met with uniform approval within the various panels were the following.

- Prohibition of the use of force is not limited to traditional kinetic weapons. Use of ICTs can indeed amount to the unlawful use of force; breach of the obligation does not necessitate use of kinetic means.
- Cyber operations resulting in physical damage or injury to human beings could qualify as use of force.
- States targeted by a cyber operation amounting to the use of force may resort to reactions recognized in customary international law of State responsibility, namely retorsion or countermeasures.
- States remain free to choose the modality for peaceful settlement of disputes involving a disagreement on the legal or factual aspects of State use of ICTs. At the same time, the principle of good faith remains applicable to the peaceful settlement of disputes arising from the State use of ICTs.

At the same time, the discussions affirmed some divergent positions on how the Charter applies to State conduct using ICTs. In order to overcome the potential challenges that could manifest as a result, the panellists deliberated on a number of proposals for future action. Accordingly, States could pursue the following actions in relation to the State conduct in cyberspace.

- States should continue sharing their national interpretations of international law, as suggested in the 2022 annual progress report of the OEWG.⁴⁴ Sharing national interpretations holds the potential to contribute to transparency and thus to confidence-building among States.
- States could consider exploring establishing capacity-building mechanism(s), enabling the development of national interpretations of international law as applicable to State use of ICTs.
- States should consider discussing the potential benefits of elaborating a broad, non-exhaustive list of criteria in relation to the legal thresholds of the use of force in the context of ICT conduct of States. International convergence on the theoretical ‘red lines’ in cyberspace would facilitate predictability in international relations and confidence among the States.
- States should continue discussing the concept of threat of force in the context of State use of ICTs.
- To facilitate clarity in relation to the scope and thresholds of the prohibition of the use and threat of force in the context of cyberspace, States could make use of focused and dedicated multilateral deliberations.
- Specifically, States could consider establishing a dedicated expert subgroup of the OEWG, seek assistance from the International Law Commission and/or resort to the mechanisms of Sixth Committee.
- States could discuss Security Council sanctions and their potential utility in the maintenance of international peace and security in relation to the ICT domain.
- To facilitate the use of peaceful settlement of disputes, the Secretary-General could continue promoting the availability of his good offices.

⁴⁴ General Assembly, A/77/275, 8 August 2022, annex.

4. References

Ago, Roberto. "Addendum - Eighth report on State responsibility by Mr. Roberto Ago, Special Rapporteur - the internationally wrongful act of the State, source of international responsibility (part 1)", Yearbook of the International Law Commission, 1980, vol. II, Part One.

Brownlie, Ian. "International Law and the Use of Force by States" (Oxford, Clarendon Oxford 1963).

Charter of the United Nations, 1945, 1 UNTS XVI.

France, "International Law Applied to Operations in Cyberspace: Paper shared by France with the Open-ended working group established by resolution 75/240", 1 December 2021, <<https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf>>.

General Assembly, A/RES/3314(XXIX), 14 December 1974.

---, A/RES/A/68/98, 24 June 2013.

---, A/RES/68/243, 9 January 2014.

---, A/RES/75/240, 4 January 2021.

---, A/AC.290/2021/CRP.2, 10 March 2021.

---, A/75/816, 18 March 2021.

---, A/76/136, 13 July 2021.

---, A/76/135, 14 July 2021.

---, A/AC.292/2022/CRP.1, 28 July 2022.

---, A/77/275, 8 August 2022.

Greenwood, Christopher. "Self-Defence", in Max Planck Encyclopedia of Public International Law (Oxford, Oxford University Press 2011), <<https://opil.ouplaw.com/display/10.1093/opil/9780199231690/law-9780199231690-e401?rskey=dtukfV&result=1&prd=O-PIL>>.

International Court of Justice, "Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)", Merits, Judgment, ICJ Reports 1986.

---, "Legality of the Threat or Use of Nuclear Weapons", Advisory Opinion, ICJ Reports 1996.

---, "Oil Platforms (Islamic Republic of Iran v. United States of America)", Judgment, ICJ Reports 2003.

International Law Commission, "Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries", Yearbook of the International Law Commission, 2001, vol. II, Part Two.

Kastelic, Andraz. "Due diligence in cyberspace: Normative expectations of reciprocal protection of international legal rights", UNIDIR, 2021.

Office for Disarmament Affairs, "Securing Our Common Future: An Agenda for Disarmament", 2018, <<https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/06/sg-disarmament-agenda-pubs-page.pdf#view=Fit>>.




Permanent Mission of Singapore to the United Nations New York, "Updated 2023 OEWG Meeting Schedule", 6 April 2023, <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/Letter_from_OEWG_Chair_6_April_2023.pdf>.

---, "Revised (Rev. 2) Paper on Draft Elements for the Development and Operationalization of a Global Intergovernmental Points of Contact Directory", 8 May 2023, <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/Chair's_Letter_8_May_2023_-_POC_directory.pdf>.

Russian Federation, "Updated Concept of the Convention of the United Nations on Ensuring International Information Security", 29 June 2023, cosponsors Belarus and Nicaragua (unofficial translation), <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/ENG_Concept_of_UN_Convention_on_International_Information_Security_Proposal_of_the_Russian_Federation_0.pdf>.

Security Council, S/RES/1718 (2006), 14 October 2006.

Shah, A. Niaz. "Self-defence, Anticipatory Self-defence and Pre-emption: International Law's Response to Terrorism", Journal of Conflict & Security Law, Spring 2007, vol. 12, no. 1 (Spring 2007).

-  @unidir
-  /unidir
-  /un_disarmresearch
-  /unidirgeneva
-  /unidir



Palais de Nations
1211 Geneva, Switzerland

© UNIDIR, 2023

WWW.UNIDIR.ORG