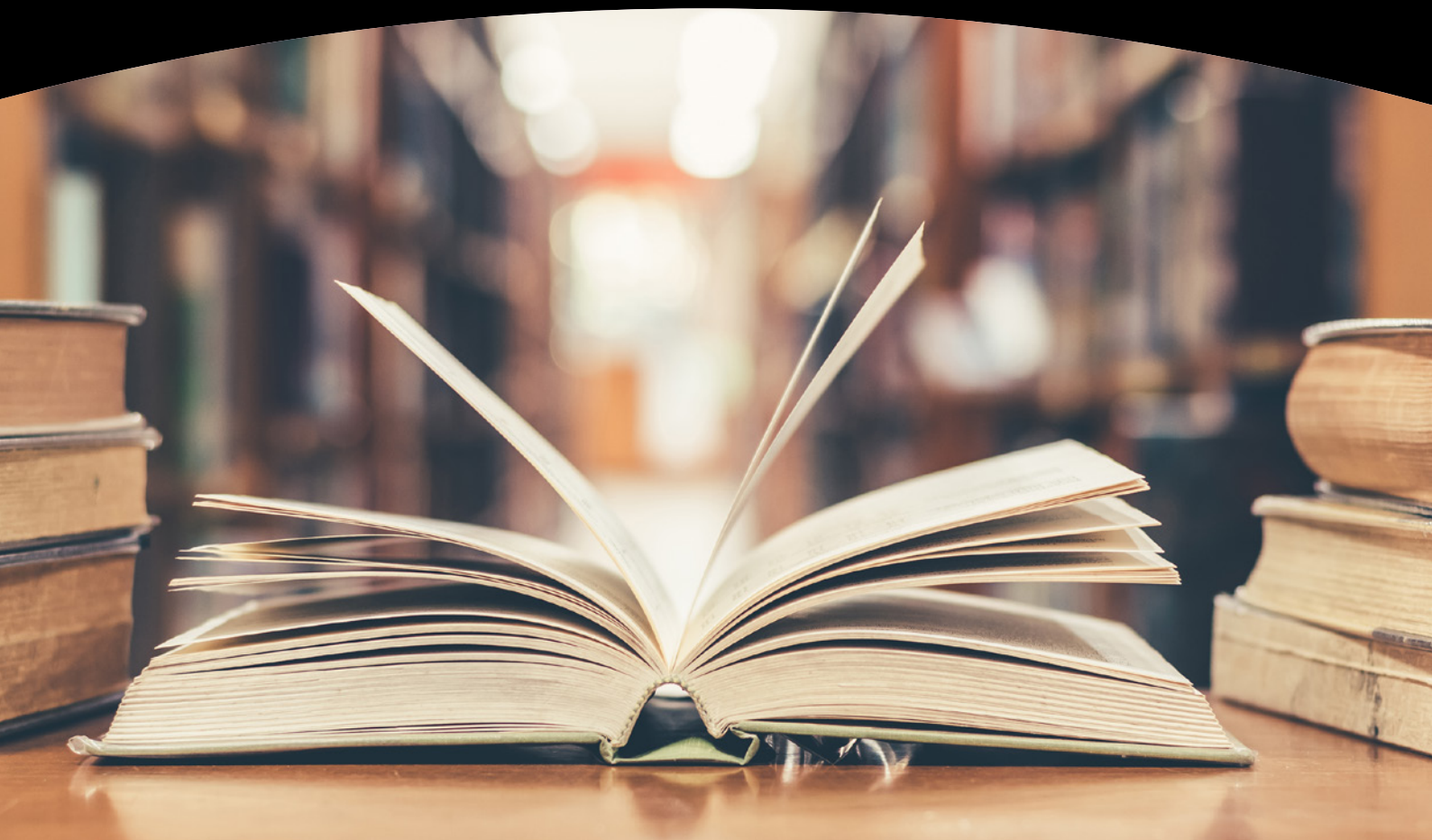
UNIDIR

A Compendium of Good Practices

Developing a National Position on the Interpretation of International Law and State Use of ICT

SECURITY AND TECHNOLOGY PROGRAMME



Contents

Acknowlegdements 3
Abbreviations 4
Executive Summary 5

1 INTRODUCTION AND CONTEXT 6

2 THE UTILITY OF A NATIONAL POSITION 8

2.1 Transparency and common understandings 8
2.1.1 Transparency on the national level 8
2.1.2 Transparency on the International level 9
2.2 National positions as a reference document 10
2.3 Fostering cooperation 10
2.4 Enhancing preparedness 11
2.5 Development of International law and promotion of compliance 11

3 THE SCOPE AND CONTENT OF A NATIONAL POSITION 13

3.1 The scope of a national position 13
3.2 The content of a national position 13

4 THE PROCESS OF DEVELOPING A NATIONAL POSITION 16

4.1 Preliminary steps 17
4.2 Capacity-building 18
4.3 Drafting a national position 19
4.4 Adoption, publication and dissemination 21

5 CONCLUSION 24

REFERENCES 25

Acknowledgements

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. Work of the Security and Technology Programme on international cybersecurity is funded by the Governments of Czechia, France, Germany, Italy, the Netherlands, Norway, Switzerland and the United Kingdom and by Microsoft. Dedicated funding for all activities leading to this compendium was provided by the United States Government.

This compendium summarizes the outcomes of a dedicated closed-door workshop; the authors wish to thank workshop participants for their active engagement and invaluable insights.

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.

Notes

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 **UNIDIR's Security and Technology Programme**. Dominique Steinbrecher and Andraz Kastelic drafted the report; Elia Duran-Smith and Edward Madziwa contributed to this report.

Cover photography © istockphoto.com/Chinnapong. Design and layout by Kathleen Morf.
www.unidir.org – © UNIDIR 2024

Abbreviations

GGE	Group of Governmental Experts
ICJ	International Court of Justice
ICT	Information and communications technology
IHL	International humanitarian law
MFA	Ministry of Foreign Affairs
MOD	Ministry of Defence
MOJ	Ministry of Justice
OAS	Organization of American States
OEWG	Open-ended Working Group

Executive Summary

This paper provides a collection of good practices and national experiences in developing a national position on the interpretation of international law in cyberspace as recorded by the States that have already developed and published one. It focuses on three aspects of a national position: utility, scope and process.

National positions can foster transparency on the national level as well as internationally. They can act as a reference document and can therefore guide bilateral engagement with international partners as well as national contributions to multilateral processes dedicated to State use of information and communications technology (ICT) in the context of international peace and security. When drafted in consultation with international partners, a national position can foster international cooperation. It can also enhance preparedness to address future cyber operations by providing national guidelines with respect to assessment, classification and response to variety of malicious cyber operations. Finally, the utility of national positions can be found in their ability to contribute to the development of international law in general. This be not only through its interpretation, but also via the potential emergence of new customary international law or codification efforts of a new legal regime.

National positions are dynamic in nature. A State's national position could initially focus on key issues as defined by that State's interest and capacity. This approach requires prioritizing certain legal areas, with the understanding that the position may evolve in the future. In particular, it may need to adapt to technological developments and evolving multilateral discussions.

To maximize their utility, national positions should prioritize the interpretation of principles and rules previously agreed by the various multilateral discussions as applicable to State use of ICT. When deciding on the content of its national position, a State could further consult existing regional approaches to the topic and the national positions of other States. Indeed, topics most frequently addressed by existing national positions include the United Nations Charter, international humanitarian law, the law of State responsibility, due diligence and international human rights law.

Last but not least, this compendium suggests 10 steps that a State could consider taking when developing its national position – starting with defining the scope of the position through, inter alia, threat landscape assessment and consideration of foreign policy priorities, and concluding with publication and dissemination of the position.

1 Introduction and context

International law is the set of rules that guide relations between sovereign States, forming a framework for their peaceful coexistence. The Charter of the United Nations is the cornerstone of the contemporary international legal order. Despite the political, economic, societal and scientific progress that have been made since its adoption in 1945, the Charter remains a vital tool for maintaining order, promoting justice, and fostering confidence and cooperation in our interconnected world.[1] Indeed, in the context of information and communications technology (ICT), States recognized that international law is "essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment".[2]

In 2013, the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security agreed that international law applies to the State use of ICT.[3] This outcome was welcomed by the United Nations General Assembly.[4] States have subsequently continued to discuss *how* international law applies to State behaviour in the digital domain.[5] To facilitate these exchanges, the Open-Ended Working Group (OEWG) on Security of and in the use of Information and Communications Technologies 2021–2025 has repeatedly called on Member States to "continue to voluntarily share their national views, which may include national statements and State practice, on how international law applies in the use of ICTs".[6]

To date, however, only 29 States have developed and published individual national positions on how international law applies to State conduct in cyberspace.[7] The relatively low numbers of national positions may be attributed to various factors, including limited awareness, resource constraints or a perception that the issue is not of immediate concern; certain States have said as much in statements to the OEWG.

The problem has been exacerbated by the lack of geographical representation among the Member States that have published a national position. More than half of the States with individual public national positions belong to the Western European and other States group.[8] Only a handful of States from other regions have published individual national positions. Recently, the African Union published a Common African Position on the Application of International Law in Cyberspace and called on its member States to consider developing and issuing individual, national views on the interpretation of international law in the context of the use of ICT.[9]

---

1 This was noted as early as 1970. General Assembly, A/RES/2625(XXV), Preamble.
2 General Assembly, A/RES/75/240.
3 General Assembly, A/68/98, 2013, para. 19.
4 General Assembly, A/RES/68/243.
5 General Assembly, A/78/265, 2023, para. 30.
6 Ibid, para. 34.
7 See UNIDIR's Cyber Policy Portal, https://www.cyberpolicyportal.org.
8 Department for General Assembly and Conference Management, "Regional Groups".
9 African Union, "Common African Position".

A greater number of individual national interpretations of international law in cyberspace and geographical diversity of national positions stating these interpretations, could foster greater confidence among States. They could also facilitate comprehensive international deliberations on common understandings of how international law applies in cyberspace.

To facilitate peer-to-peer capacity-building and support United Nations Member States in their multilateral engagements on how international law applies in cyberspace, UNIDIR's Security and Technology Programme set out to collect good practices and lessons learned from the States that have developed and published their national interpretation positions. The research team collected the data through a dedicated workshop, held in Geneva on 18 January 2024, that focused on the **utility** of a national position, its **scope** and its development **process**.

This compendium is based on the insights shared by the representatives of the 19 Member States that attended the workshop.[10] This is, two-thirds of the States with an existing position at the time of writing, and represents a diverse collection of the lessons and good practices identified during the workshop discussions.

10 The 19 States were Australia, Brazil, Canada, Czechia, Estonia, Finland, France, Germany, Italy, Kenya, the Netherlands, Norway, Pakistan, Poland, the Russian Federation, Singapore, Sweden, Switzerland and the United States of America.

2 The utility of a national position

This section highlights various, interrelated reasons in favour of developing and publishing a national position on the interpretation of international law in cyberspace.

Utility of a national position

- Promotes transparency and common understandings
  - > National level
  - > International level
- Serves as a reference document for international dialogue
- Fosters cooperation among different stakeholders
- Enhances national preparedness to address malicious cyber operations
- Provides a platform to further clarify and contribute to the development of international law and promote its compliance

2.1 Transparency and common understandings

Among the States that have already done so, a commonly expressed rationale for developing and publishing an individual national position is the need to enhance **transparency** on the national and international levels. Transparency in turn facilitates the development of **common understandings** on how international law applies in cyberspace.

2.1.1 Transparency on the national level

The process of developing a national position contributes to the identification of relevant national stakeholders that are, or should be, engaged in the discussion on international law in cyberspace and relevant existing national efforts.[11] It also provides national structures with an opportunity to reflect on complex legal issues and to clarify their understandings of the law in the domain of ICT.

The process of developing a national position inherently includes an element of capacity-building[12] and thus promotes knowledge-sharing among the domestic stakeholders. Additionally, the process promotes national dialogue and cooperation, and it minimizes the potential for the duplication of efforts.

---

11 In some cases, institutional constraints include the distribution of expertise in a way that is difficult to articulate, and thus the need for further internal dialogue which can be fostered through the process of developing a national position. See, in this regard, OAS, "Improving Transparency", paras 18–19.

12 See Section 4.2 below.

Last but not least, if the process culminates in the adoption of a position, the outcome is a common national platform. This ensures consistency across the different agencies and departments in their efforts related to international cybersecurity, and therefore contributes to the State's internal coherence in the interpretation of the existing international legal framework.

2.1.2 Transparency on the International level

Publishing or sharing a national position also constitutes an exercise in transparency on the international level. It promotes confidence by advancing legal clarity and certainty and, thus, predictability in international relations. It can reduce the risks of misunderstandings and the potential for escalation in international relations, thereby aiding common efforts towards international peace and security.

Elaboration of a national interpretation of international law helps with identifying sensitive or controversial issues and, by establishing so-called red lines, communicates legal expectations of the behaviour of other States. Some workshop participants suggested such national positions can therefore have a deterrent function.

Moreover, transparency in relation to the international community could facilitate international dialogue. National positions can contribute to the development of **common international understandings** on how international law applies to cyberspace and the identification of situations to which international law applies. A national position can also be a valuable instrument for identification of areas of international convergence and divergence, and pathways to address potential gaps.

United Nations Members States have found similar consensus on transparency in various multilateral processes. For example, the 2019–2021 GGE on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security stated that international law is key to enhancing confidence among States.[13] It also acknowledged that discussion and exchanges of views by States on how specific rules and principles of international law apply to the use of ICTs is essential for "deepening common understandings, avoiding misunderstandings and increasing predictability and stability".[14]

In the same vein, the 2019–2021 OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security recommended in its final report that States continue to develop their national views and assessments on how international law applies to their use of ICTs and to voluntarily share such positions and practices. Its rationale was that deepening common understanding on the issue would contribute to building consensus within the international community.[15]

13 General Assembly, A/76/135, para. 69.
14 General Assembly, A/76/135, paras 72–73.
15 General Assembly, A/75/816, paras 36–37.

Similar views have also been clearly reflected in existing national positions.[16] Moreover, improved transparency in the application of international law in cyberspace has been stressed as the clear objective for regional projects.[17]

Finally, according to the 2019–2021 GGE and the 2019–2021 OEWG, transparency measures such as the voluntary exchange of views constitute **confidence-building measures**.[18] This has also been reaffirmed at the regional level, for example in the list of cooperation and confidence-building measures in cyberspace composed by the Inter-American Committee against Terrorism of the Organization of American States (OAS/CICTE),[19] as well as by other stakeholders.[20]

2.2 National positions as a reference document

National positions have proven to be useful as reference documents or "road maps" for enhancing international dialogue by guiding governments' engagements and statements in international multilateral processes, regional dialogues and bilateral interactions. At the same time, they are considered as dynamic documents that may benefit from the continuous discussion at the international level and from capacity-building activities within these settings.

2.3 Fostering cooperation

Relatedly, the development of national positions can foster engagement among States and other relevant stakeholders in the field of ICTs. This is particularly the case when the State drafting a position consults with different stakeholders and international partners, seeking guidance, assistance or feedback. In turn, this could open new avenues for bilateral, regional and international cooperation and technical assistance or capacity-building efforts.[21] Effective cooperation has a prominent role in the framework of responsible State behaviour in the use of ICT and has been identified as essential for peaceful and stable cyberspace.[22]

---

16 See, for example, African Union "Common African Position", para. 4; Canadian Government, "International Law Applicable in Cyberspace", para. 5; Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position", para. 5; Chinese Ministry of Foreign Affairs, "China's Positions"; Czech Ministry of Foreign Affairs, "Position Paper", p. 1; Danish Government, "Denmark's Position Paper", p. 2; French Ministry of Armed Forces, "International Law Applied to Operations in Cyberspace", p. 1; German Federal Government, "On the Application of International Law in Cyberspace", p. 2; Irish Department of Foreign Affairs, "Position Paper", para. 2; Japanese Ministry of Foreign Affairs, "Basic Position", p. 2; Netherlands Government, "International Law in Cyberspace", p. 1; Polish Ministry of Foreign Affairs, "Republic of Poland's Position", p. 1; Swedish Government Offices, "Position Paper", p. 1; United Kingdom Foreign, Commonwealth and Development Office, "Application of International Law to States' Conduct in Cyberspace"; General Assembly, A/76/136, p. 18 (Brazil), pp. 23–24 (Estonia), p. 53 (Kenya), p. 136 (United States); Egan, "International Law and Stability in Cyberspace", pp. 6–7.

17 OAS, "Improving Transparency", para. 1.

18 General Assembly, A/76/135, paras 82ff; General Assembly, A/75/816, paras 41ff.

19 OAS/CICTE, "List of Consolidated Cooperation and Confidence-building Measures in Cyberspace", para. 8.

20 See, for example, Oxford Institute for Ethics, Law and Armed Conflict, "ELAC Intervention"; Moynihan, "The Vital Role of International Law".

21 For example, during the development of the common African position, a capacity-building programme was organized for diplomats, experts and government lawyers in the region, which was funded and co-organized with the Government of Canada. See Helal, "The Common African Position".

22 General Assembly, A/76/135, para. 5.

2.4 Enhancing preparedness

By clarifying a State's interpretation of thresholds of acceptable State use of ICTs under international law, a national position not only contributes to international dialogue but can also enhance national preparedness to respond to malicious cyber operations. The development of a national position can contribute to the State's preparedness by providing a clear framework for assessing, classifying and responding to malicious cyber operations.

2.5 Development of International law and promotion of compliance

The clarification and exchange of States' views can contribute to the development of international law in different ways.

First, the process of drafting a national position can provide a platform to further clarify and contribute to the **development of general rules of international law**. Second, national positions can contribute to the **interpretation of international law** by defining how existing treaty law and the rules of customary international law apply and can be extended to the cyber domain by means of interpretation.[23]

Third, national positions could themselves contribute to the development of **customary international law**, one of the main sources of international law.[24] The emergence of customary rules requires the concurrent existence of a general State practice and an acknowledgement by States that this particular practice is guided by the existence of a legal rule or, in other words, a sense of legal obligation. National positions on international law in cyberspace can serve as evidence of one of the elements of customary international law: they can be seen as the expression of opinions by a State in regard to international rights and obligations in cyberspace or can be interpreted as evidence of corresponding practice of a State. When they reach a high level of international adoption, national positions can therefore serve as a basis for the development of international law. More specifically, they can contribute to the formation of new rules of customary international law in the context of State use of ICT.

In addition, some States currently maintain that cyber threats to international peace and security necessitate an international response in a form of a **new, dedicated legal regime**.[25] For example, a number of States co-sponsored a OEWG paper that outlined a concept for a United Nations convention on ensuring international information security.[26] In addition to facilitating international dialogue on how existing international law applies to cyberspace, national positions would enable the States to contribute to the discussion on "whether gaps in common understandings exist on how international law applies"[27] and evaluate the proposals as above.

---

23 For further discussions on the concept of "dynamic" or "evolutionary" interpretation of international law, see Vienna Convention on the Law of Treaties, Article 31(3)(b); ICJ, "Costa Rica v. Nicaragua", p. 213, para. 66; Marco Roscini, *Cyber Operations and the Use of Force*, p. 19ff.

24 See Statute of the International Court of Justice, Article 38(b).

25 General Assembly, A/77/275, annex.

26 Russian Federation et al., "Updated Concept".

27 General Assembly, A/77/275, annex, para. 15(b)(i)–(ii) and International Law section, Recommended Next Steps 2.

Last but not least, some States suggest that national positions contribute to the **strengthening of the rule of international law** and promote compliance.[28]

However, as highlighted above, for this to materialize requires engagement by a broader range of States, diverse voices and a better geographical representation in the international dialogue on how international law applies to the State use of ICT. As stressed by the African Union in its common African position and in line with the principle of sovereign equality, "[a]ll States have an equal right to participate in the articulation of rules of international law that apply in cyberspace and the views of all States have equal weight and value in this process".[29]

28 See, for example, Polish Ministry of Foreign Affairs, "Republic of Poland's Position", p. 1.

29 African Union, "Common African Position", para. 6. See also in this regard discussion in the realm of the OAS: OAS, "Improving Transparency", p. 17. See also EU Cyber Direct, "Toward an EU Position", p. 2.

3 The scope and content of a national position

By summarizing the deliberations of the workshop, this section provides guidance on the scope and content of a national position on the interpretation of international law in cyberspace.

3.1 The scope of a national position

The workshop discussions emphasized the dynamic nature of national positions. A position therefore does not need to be exhaustive but should instead focus on the most important issues as defined by the individual State based on its national priorities and capacity. This necessitates prioritization of legal areas to be addressed initially, while national positions can develop over time through a continued improvement process. A State could choose to address, for example, the most contentious legal issues in the context of State use of ICTs; those that are considered more relevant given the current threat landscape; or topics that are aligned with its foreign policy priorities. The scope of the national position may also depend on the desired impact (various aspects of the utility of a national position are discussed in section 2).

Existing national positions refer to their non-exhaustive character.[30] Arguments for this are based on the fact that positions may eventually need to adapt in order to address rapid technological developments or to enable continuing and meaningful engagement in the evolving multilateral discussions.[31] Indeed, some States have already complemented or updated their initial national positions on international law in cyberspace.

3.2 The content of a national position

Workshop discussions indicated that the structure of a national position should clearly reflect its purpose. Accordingly, a national position would probably benefit from an introduction and conclusion, not only to frame the content but also to provide its purpose. This could include the backdrop to the development of the national position on the interpretation of international law, such as the specific threat landscape and the need for transparency, preparedness and cooperation in this regard.

---

30 See, for example, African Union, "Common African Position", para. 10; Canadian Government, "International Law Applicable in Cyberspace", para. 7; Czech Ministry of Foreign Affairs, "Position Paper", p. 1; Danish Government, "Denmark's Position Paper"; Irish Department of Foreign Affairs, "Position Paper", para. 3; Italian Ministry of Foreign Affairs and International Cooperation, "Italian Position Paper", p. 3; Swiss Federal Department of Foreign Affairs, "Switzerland's Position Paper", p. 1; United Kingdom Foreign, Commonwealth and Development Office, "Application of International Law to States' Conduct in Cyberspace"; General Assembly, A/76/136, p. 18 (Brazil), p. 75 (Romania) p. 85, para. 21 (Singapore); Koh, "International Law in Cyberspace", p. 3.

31 See, for example, African Union, "Common African Position", para. 10; Canadian Government, "International Law Applicable in Cyberspace", para. 7; Danish Government, "Denmark's Position Paper"; General Assembly, A/76/136, p. 85, para. 20 (Singapore); Swedish Government Offices, "Position Paper", p. 1, among others.

The content of the existing national positions is diverse, which is reflected in the heterogenous positions expressed in the relevant multilateral discussions on international law in cyberspace. What is more, recent international discussions suggest that some Member States either question or are cautious about the application of certain bodies of law or specific rules.

Nonetheless, the representatives of United Nations Member States participating at the workshop identified appropriate topics for national positions. These bodies of law, listed below in no particular order, reflect the focused discussions of the 2021–2025 OEWG and enjoyed varying degree of support during the workshop.

- **The applicability of international law** to cyberspace and key concerns in this regard
- **United Nations Charter**: most participants stressed that national positions should address issues under the United Nations Charter, including:
  - State sovereignty
  - The principle of non-intervention
  - The prohibition of the threat and use of force
  - The peaceful settlement of disputes
- Other branches of international law
  - International human rights law
  - International humanitarian law
  - The law of neutrality
- **The law of State responsibility**, with particular focus on
  - Attribution
  - Countermeasures
  - Due diligence
- Other issues:
  some participants opined that States should also address the role of private actors, international cooperation, capacity-building, and the link with cybercrime and technological development.

When deciding on the content of the national position, most States sought inspiration in the outcomes of the multilateral discussions on international law in cyberspace, in regional approaches to the topic and in the national positions of other States.

Indeed, the list of topics above closely follows those identified by the relevant multilateral processes as having central importance.[32] Moreover, an analysis of the 30 positions publicly available as of March 2024 indicates congruence on the issues that should be dealt with in a national position:[33]

All current national positions refer to the general topic of the applicability of international law in cyberspace

28 national positions refer to State sovereignty

27 national positions address the applicability of international humanitarian law (IHL) to cyber operations (some referring to the topic more generally and others dealing in depth with issues such as conflict classification, the notion of attack under IHL and the application of the principles on the conduct of hostilities)

The vast majority of positions discuss the law on State responsibility, with **26** addressing in particular the complex topic of attribution and **25** discussing countermeasures

26 national positions address the principle of non-intervention and the prohibition of the use of force

24 national positions address the right to self-defence under the United Nations Charter as well as the issue of due diligence

23 positions refer to the application of international human rights law in cyberspace

Other topics widely addressed by the existing national positions are the peaceful settlement of disputes, acts of retorsion, the plea of necessity and the law of neutrality.

---

32 The specific topics are: (a) sovereign equality and State sovereignty; (b) the principle of non-intervention; (c) the peaceful settlement of disputes; (d) the prohibition of the threat and use of force and the inherent right of States to take measures consistent with international law and as recognized in the United Nations Charter; (e) respect for human rights and fundamental freedoms; (f) due diligence; (g) the law on State responsibility; and (h) that international humanitarian law applies only in situations of armed conflict, recalling the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction. See General Assembly, A/70/174, paras 26–28; General Assembly, A/76/135, paras 70–71.

33 See all the publicly available national positions on UNIDIR's Cyber Policy Portal, https://cyberpolicyportal.org.

4 The process of developing a national position

This section summarizes the workshop outcomes related to the process of developing a national position on the interpretation of international law in cyberspace. In particular, it outlines how to develop a national position and who should be involved and identifies the key lessons learned by States that have developed a national position.

The following **10 steps** emerged as good practices related to the process of developing a national position. The list represents a set of recommendations which can be used as guidance throughout the process of development of a national position; they should not be treated as rigid requirements for success and should be adapted to each specific national context.

Preliminary steps	1	**WHAT?** Scope
	2	**WHO?** Stakeholders involved
	3	**HOW?** Key institutional steps
	4	**WHEN?** Plan
Capacity-building	5	Capacity-building
Drafting a national position	6	Background resources and interpretation tools
	7	Collaborations and consultations
	8	General drafting principles
Adoption, publication and dissemination	9	Adoption
	10	Publication and dissemination

4.1 Preliminary steps

1

WHAT? Define the scope:

A. Identify the **target audience** and the **desired impact** of the national position.

B. Identify **key questions** that the national position should address.

C. Define the **main areas of international law** that the national position should address. As stressed in sections 2 and 3, in defining the content of its national position a State can draw inspiration from other States' positions and the discussions within multilateral and regional processes, among other sources.

D. Within the preliminary steps, and to better understand the framework in which the national position will be developed, a State could also take the following preliminary actions:

> Define the **threat landscape** in the State, to be able to shape the position accordingly.

> Identify the **national security and foreign policy priorities** of the State on international law topics and cybersecurity issues that should necessarily be included in the position or on which the State would require an in-depth analysis.

2

WHO? Define the stakeholders involved:

A. **Identify the agencies and departments** that should be involved in the process.

B. **Allocate the roles** and responsibilities among the different stakeholders involved.

C. **Identify the penholder** and create a **mandate** for the agency or department taking the lead in the drafting of the position. According to some States participating in the workshop, the establishment of a small drafting group proved to be a good practice as did the involvement of national legal advisers or experts. In addition to legal experts, and given the complexities of cyberspace, States could consider involving a broad range of experts with technical, practical and operational experience.

D. **Establish regular consultations with and updates** to the larger group of stakeholders.

An analysis of the existing national positions indicates that they could be prepared by, or in consultation with, the Ministry of Foreign Affairs (MFA),[34] the Ministry or Department of Defence (MOD/DOD)[35] and/or the Ministry of Justice (MOJ) or Attorney-General's Office.[36] In many cases, the process also involved other ministries, departments or agencies, such as the National Cybersecurity Agency.[37]

34 See Canadian Government, "International Law Applicable in Cyberspace"; Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position"; Finnish Ministry for Foreign Affairs, "Finland Published its Positions"; Irish Department of Foreign Affairs, "Position Paper"; Japanese Ministry of Foreign Affairs, "Basic Position"; New Zealand Foreign Affairs & Trade, "The Application of International Law", p. 4; Polish Ministry of Foreign Affairs, "Republic of Poland's Position"; Swiss Federal Department of Foreign Affairs, "Switzerland's Position Paper".

3

HOW? Identify key institutional steps:

A. Anticipate the requirements of the **institutional context** with which the drafting of the national position will have to comply. For example, necessary reviews and approvals by specific authorities, agencies or public powers, and the definition of which authority (or authorities) will adopt the position.

B. Ensure the allocation of an appropriate and dedicated **budget** to assure the necessary financial and human resources.

4

WHEN? Formulate a plan:

Establish a clear **timeline** for the development of the national position, with precise deadlines. To avoid unexpected delays and considering the number of stakeholders involved, the timeline should factor in processes such as the time needed for internal and external consultations. It should also accommodate the time for its revision and approval.

4.2 Capacity-building

5

Capacity-Building

Building the capacity of those involved in the development of the national position is a recommended cross-cutting step. It facilitates provision of the legal and technical expertise required for a knowledgeable interpretation of international law and for development of the State's views on how it applies to cyberspace, considering all the necessary background and existing discussions. Capacity-building can take the form of exercises, scenario-based workshops, training programmes, conferences, etc. It can also benefit from bilateral, regional and international cooperation. Capacity-building activities should follow the principles of capacity-building as agreed by the 2019–2021 OEWG.[38]

States could consider capacity-building activities for all the involved stakeholders. This will not only facilitate development of the position but contribute to confidence among various relevant national entities and promote internal cohesion.

35 See, for example, French Ministry of Armed Forces, "International Law Applied to Operations in Cyberspace"; Ney, "Remarks".

36 Wright, "Cyber and International Law"; Braverman, "International Law in Future Frontiers"; Schöndorf, "Israel's Perspective".

37 See, for example, Czech Ministry of Foreign Affairs, "Position Paper", p. 1; German Federal Government, "On the Application of International Law in Cyberspace"; Italian Ministry of Foreign Affairs and International Cooperation, "Italian Position Paper", p. 3; Netherlands Minister of Foreign Affairs, Letter; Musæus, "Norway's Position Paper"; Australian Government, "Australia's Position".

38 General Assembly, A/75/816, para. 56.

4.3 Drafting a national position

6

Background resources and interpretation tools

Varied sources can be a useful resource to be consulted during the drafting process. They may include the following:

A. **Final and annual progress reports from United Nations multilateral processes**, such as the GGEs and the OEWGs, can be useful resources to trigger the development, drafting and publishing of a position, and as a baseline to establish the timeline of these efforts. In addition, all other relevant documents submitted to those processes (such as working papers, non-papers, background documents and presentations) are also relevant sources. Background documents from regional processes can also prove very useful for the identification of relevant regional perspectives.

B. **Academic literature and case law**

> Academic literature can be a useful source for the understanding and interpretation of the rules and principles of international law. Further, some existing national positions point to experts reports and studies, position papers by relevant international organizations and institutions (such as, for example, the International Committee of the Red Cross), and academic projects as relevant reference material.[39]

> International case law, in particular from the International Court of Justice (ICJ), was highlighted as useful and is indeed widely featured in a number of existing national positions.[40]

C. **Other national positions** were referred to as useful inspiration when drafting a national position.[41]

Some States note in their national positions that, in formulating their views, the starting point was the traditional **sources of international law** as enshrined in Article 38 of the ICJ Statute.[42] Many other normative instruments are referenced in the existing national positions, such as the International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts. Further, some national positions rely on **treaty interpretation rules**[43] to ascertain the applicability and relevance of the provision in cyberspace.[44]

---

39 See, for example, Czech Ministry of Foreign Affairs, "Position Paper", p. 1; Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position", para. 6; German Federal Government, "On the Application of International Law in Cyberspace", pp. 2, 16; Japanese Ministry of Foreign Affairs, "Basic Position", p. 1; General Assembly, A/76/136, p. 18 (Brazil); Egan, "International Law and Stability in Cyberspace", p. 6.

40 For example, some of the most cited cases and advisory opinions of the ICJ in available national positions include, among others, ICJ, "Nicaragua v. United States of America"; ICJ, "Democratic Republic of the Congo v. Uganda"; ICJ, "Corfu Channel Case"; ICJ, "Legality of the Threat or Use of Nuclear Weapons".

41 See all the publicly available national positions on UNIDIR's Cyber Policy Portal, https://cyberpolicyportal.org.

42 Netherlands Government, "Appendix: International Law in Cyberspace", p. 1; General Assembly, A/76/136, p. 18 (Brazil).

43 Notably, Article 31 of the Vienna Convention on the Law of the Treaties.

44 See, for example, Schöndorf, "Israel's Perspective", p. 397; German Federal Government, "On the Application of International Law in Cyberspace", p. 16.

7

Collaborations and consultations

The interactive nature of the process has been highlighted by several States as very relevant. Both internal and external collaboration is considered to be a good practice during the process of developing a national position.

A. **Inter-agency/departmental consultations** assist with the identification of and engagement with all relevant stakeholders across the government in a regular dialogue on contributions to the development of the national position and on building internal coherence. An initial draft outline could be shared with the relevant stakeholders for initial feedback and agreement on the scope and content; this can be followed by subsequent periodic rounds of consultations. The usual agencies/departments involved in the development include the MFA, the MOD/DOD, the MOJ and the Attorney-General's Office, and cybersecurity agencies, among others. Regular consultations with senior officials could also facilitate later approval of the position.

B. Consultations/cooperation with **other States** in bilateral, regional or international settings could also prove useful as highlighted by multilateral processes and some States in their national positions.[45]

C. Consultations on the draft position could be held with **other stakeholders**, both nationally and internationally and including academia, the private sector and non-governmental organizations, among others. Some states expressly mention consultations with different stakeholders in their national positions.[46]

45 See, for example, General Assembly, A/76/135, para. 72; Canadian Government, "International Law Applicable in Cyberspace", para. 53; Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position", para. 6; Czech Ministry of Foreign Affairs, "Position Paper", p. 1; Japanese Ministry of Foreign Affairs, "Basic Position", p. 1; Netherlands Government, "Appendix: International Law in Cyberspace", p. 1; Wright, "Cyber and International Law".

46 Canadian Government, "International Law Applicable in Cyberspace", para. 53; Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position", para. 6; Czech Ministry of Foreign Affairs, "Position Paper", p. 1; General Assembly, A/76/136, p. 30 (Estonia); Wright, "Cyber and International Law".

8

General drafting principles

When drafting the national positions, States could consider the following principles:

> **Accessibility:**
National positions should be drafted using accessible language considering the target audience and taking account of its wide dissemination.

> **Clarity:**
Positions should be clear and assertive since ambiguity in the presentation of views regarding certain rules can lead to misinterpretation. This does not mean that States cannot highlight unsettled issues on which further study is needed to clarify their interpretation. The inclusion of key messages in each topic and the definition of specific terms can be highlighted as a good practice.

> **Include examples:**
Linked to the point on clarity, a good practice to enhance the precision of the State's views and better illustrate the interpretation is to include practical examples of what the application of certain international law rules would entail in practice. These can be hypothetical or abstract examples.

4.4 Adoption, publication and dissemination

9

Adoption

The national position should be adopted or approved by a designated authority, following the defined institutional process. As mentioned above, early clarity on which entity will adopt and how has been highly recommended by some of the States that have already developed a national position.

For example, some States opted to submit the position to the legislative power,[47] while other national positions needed to be adopted by a specific institution (for example, the Council of Ministers).[48]

47 Netherlands Minister of Foreign Affairs, Letter. In the particular case of the Netherlands, the mandate to develop a national position came directly from the Parliament. Thus, the MFA in conjunction with the MOD, the MOJ, and the Ministry of the Interior and Kingdom Relations addressed a letter to the Parliament to inform it about the position on international law in cyberspace, annexing it as an appendix to the letter. In the case of Finland, for example, the State expressed the view that the content and rationale of the national position, which was prepared by the MFA in consultation with other relevant authorities, was submitted to the Foreign Relations Committee of the Parliament although not formally enacted by that organ.

48 See, for example, Polish Ministry of Foreign Affairs, "Republic of Poland's Position". In the case of Poland, on the initiative of the MFA, the Council of Ministers adopted Poland's position on the application of international law in cyberspace.

10

Publication and dissemination

Some States participating in the workshop highlighted the importance of **publishing** the national positions,[49] which would indeed facilitate transparency and legal certainty.

Many States submitted their positions to the 2019–2021 GGE and so they were included in the Official Compendium of voluntary national contributions on how international law applies to the State use of ICTs.[50]

Some States organized special publication events or presented their positions during academic conferences.[51] Some released their positions through their official channels[52] (usually through the official website of the MFA[53] or MOD).[54] Some submitted their position to the United Nations Office of Disarmament Affairs[55] or directly to the OEWG.[56] And some published the position in a law journal.[57]

49 Canadian Government, "International Law Applicable in Cyberspace", para. 4; Musæus, "Norway's Position Paper", among others.

50 General Assembly, A/76/136.

51 See, for example, Estonian President, "International Law Applies Also in Cyber Space"; United States Naval War College, "Disruptive Technologies"; Wright, "Cyber and International Law"; Braverman, "International Law in Future Frontiers"; Koh, "International Law in Cyberspace"; Egan, "International Law and Stability in Cyberspace"; Ney, Remarks.

52 Australian Government, "Australia's Position"; German Federal Government, "On the Application of International Law in Cyberspace"; Netherlands Government, "Appendix: International Law in Cyberspace", p. 1; Swedish Government Offices, "Position Paper".

53 See, for example, Canadian Government, "International Law Applicable in Cyberspace"; Chinese Ministry of Foreign Affairs, "China's Positions"; Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position"; Czech Ministry of Foreign Affairs, "Position Paper"; Finnish Ministry for Foreign Affairs, "Finland Published its Positions"; Italian Ministry of Foreign Affairs and International Cooperation, "Italian Position Paper"; Japanese Ministry of Foreign Affairs, "Basic Position"; New Zealand Foreign Affairs & Trade, "The Application of International Law", p. 4; Polish Ministry of Foreign Affairs, "Republic of Poland's Position"; Swiss Federal Department of Foreign Affairs, "Switzerland's Position Paper".

54 French Ministry of Armed Forces, "International Law Applied to Operations in Cyberspace".

55 Pakistan Mission to the United Nations, "Pakistan's Position".

56 Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position"; French Ministry of Armed Forces, "International Law Applied to Operations in Cyberspace".

57 Danish Government, "Denmark's Position Paper"; Lehto, "Finland's Views"; Schöndorf, "Israel's Perspective"; Musæus, "Norway's Position Paper"; Engdahl, "Sweden's Position Paper".

10

Publication and dissemination (cont.)

Moreover, States have also emphasized the need to invest in **socializing** the national positions both internally and externally. Specifically, the following relevant good practices have been suggested in order to extend the reach of the national position to different stakeholders:

A. Draft the national position using accessible language and content.

B. Develop a communication plan. Prepare an informal and accessible summary of the position or other communication materials such as drafting a short blogpost explaining its main content.

C. Organize briefings with different (national and international) stakeholders to present the position and raise awareness across the different sectors.

D. Translate the national position into different languages (e.g., United Nations official languages).

E. Share and disseminate the national position in relevant international forums, such as at the multilateral processes or regional endeavours in the field of ICTs. In fact, the OEWG has repeatedly encouraged States to share their views.[58]

F. The timing of the publication of the position can influence its reception by some stakeholders, in particular in the international arena. Considering the schedule of the relevant multilateral processes could enhance the discussions on the position in those forums.

58 General Assembly, A/76/135, para. 73.

5 Conclusion

This compendium of good practices outlines the possible utility of a national position on the interpretation of international law in cyberspace, makes suggestions on the scope and content, and provides examples of good practice in the process of developing a position. However, as indicated in the workshop, States face several challenges related to the development of a position.

Capacity has been stressed as an issue by many of the States that had drafted a national position and has been highlighted by the literature as one of the factors that can preclude some States from developing their positions.[59] This includes the available legal, policy and technical capacity of States, the different levels of understanding among the involved stakeholders, in addition to constraints in terms of time and human and economic resources.

A lack of the necessary political will to develop a national position has also been stressed as a reason for the limited number of States sharing their views on the application of international law in cyberspace.[60] Having the political will from a high level of government can be decisive, not only for the final adoption of the position, but also in the prioritization and allocation of sufficient resources to its development.

The highlighted utility of developing and sharing States' views on the application of international law in cyberspace can only be truly evidenced if an extended number of States with a well-balanced geographical representation use their voices and substantively engage in the discussions. Therefore, as already stressed by multilateral processes,[61] as well as by regional organizations[62] and States,[63] there is a pressing need to raise awareness, build capacity as well as foster international cooperation for an inclusive and meaningful conversation. It is worth noting that capacity-building and international cooperation are pillars of the framework of responsible State behaviour in the use of ICTs developed in United Nations processes. This can include bilateral inter-State initiatives, regional or international capacity-building efforts, and engagement with multiple stakeholders, including international organizations, civil society, academia and the private sector.[64]

This compendium aims at assisting these efforts by systematizing good practices into a useful framework that could ease the decision to develop a national position and the process of drafting it.

---

59 See, for example, Hollis, "A Brief Primer".

60 OAS, "Improving Transparency", para. 21.

61 General Assembly, A/75/816, paras 37–39.

62 African Union, PSC/PR/COMM.1196 (2024), para. 8; OAS, "Improving Transparency", para. 13.

63 Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position", para. 5; Canadian Government, "International Law Applicable in Cyberspace", para. 6; Pakistan Mission to the United Nations, "Pakistan's Position", paras 20–21; General Assembly, A/76/136, p. 53 (Kenya).

64 African Union, PSC/PR/COMM.1196 (2024), para. 8.

References

African Union, Peace and Security Council, "Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace", 29 January 2024, https://papsrepository.africa-union.org/bitstream/handle/123456789/2022/1196%20AU%20Common%20Position%20Adopted%20Version%20-%20EN.pdf?sequence=11&isAllowed=y.

African Union, Peace and Security Council, Communiqué, PSC/PR/COMM.1196 (2024), 29 January 2024, https://papsrepository.africa-union.org/bitstream/handle/123456789/2022/1196%20AU%20Common%20Position%20Adopted%20Version%20-%20EN.pdf?sequence=11&isAllowed=y.

Australian Government, "Australia's Position on How International Law Applies to State Conduct in Cyberspace", 2020, https://www.dfat.gov.au/international-relations/themes/cyber-affairs-and-critical-technology.

Braverman, Suella, United Kingdom Attorney-General, "International Law in Future Frontiers", 19 May 2022, https://www.gov.uk/government/speeches/international-law-in-future-frontiers.

Canadian Government, "International Law Applicable in Cyberspace", April 2022, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng.

Chinese Ministry of Foreign Affairs, "China's Positions on International Rules-Making in Cyberspace", October 2021, https://www.fmprc.gov.cn/wjb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/202110/t20211012_9552671.shtml.

Chinese Ministry of Foreign Affairs, "China's Views on the Application of the Principle of Sovereignty in Cyberspace", December 2021, https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf.

Costa Rican Ministry of Foreign Affairs, "Costa Rica's Position on the Application of International Law in Cyberspace", 21 July 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf.

Czech Ministry of Foreign Affairs, "Position Paper on the Application of International Law in Cyberspace", 27 February 2024, https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf.

Danish Government, "Denmark's Position Paper on the Application of International Law in Cyberspace", *Nordic Journal of International Law*, Vol. 92, 4 July 2023, https://brill.com/view/journals/nord/92/3/article-p446_007.xml.

Department for General Assembly and Conference Management, "Regional Groups of Member States", https://www.un.org/dgacm/en/content/regional-groups.

Egan, Brian J., "International Law and Stability in Cyberspace", 10 November 2016, https://www.law.berkeley.edu/wp-content/uploads/2016/12/BJIL-article-International-Law-and-Stability-in-Cyberspace.pdf.

Engdahl, Ola, "Sweden's Position Paper on the Application of International Law in Cyberspace", *Nordic Journal of International Law*, Vol. 92, No. 3 (2023), https://brill.com/view/journals/nord/aop/article-10.1163-15718107-20230004/article-10.1163-15718107-20230004.xml.

Estonian President, "International Law Applies Also in Cyber Space", 29 May 2019, https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.

EU Cyber Direct, "Toward an EU Position on the Application of International Law in Cyberspace", 8 June 2023, https://eucyberdirect.eu/research/toward-an-eu-position-on-the-application-of-international-law-in-cyberspace.

Finnish Ministry for Foreign Affairs, "Finland Published its Positions on Public International Law in Cyberspace", 15 October 2020, https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c-6d85?t=1603097522727.

French Ministry of Armed Forces, "International Law Applied to Operations in Cyberspace", 9 September 2019, https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf.

General Assembly, Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, A/RES/2625(XXV), 20 October 1970, https://undocs.org/A/RES/2625(XXV).

General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013, https://undocs.org/A/68/98.

General Assembly, ''Developments in the Field of Information and Telecommunications in the Context of International Security", A/RES/68/243, 27 December 2013, https://undocs.org/A/RES/68/243.

General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, https://undocs.org/A/70/174.

General Assembly, ''Developments in the Field of Information and Telecommunications in the Context of International Security", A/RES/75/240, 31 December 2020, https://undocs.org/A/RES/75/240.

General Assembly, Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/75/816, 18 March 2021, https://undocs.org/A/75/816.

General Assembly, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, https://undocs.org/A/76/135.

General Assembly, "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States", A/76/136, 31 July 2021, https://undocs.org/A/76/136 (containing the views of Australia, Brazil, Estonia, Germany, Japan, Kazakhstan, Kenya, Netherlands, Norway, Romania, the Russian Federation, Singapore, Switzerland, the United Kingdom, and the United States of America)

General Assembly, Report of the Open-Ended Working Group on Security of and in the use of Information and Communications Technologies 2021–2025, A/77/275, 8 August 2022, https://undocs.org/A/77/275.

General Assembly, Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/78/265, 1 August 2023, https://undocs.org/A/78/265.

German Federal Government, "On the Application of International Law in Cyberspace", Position Paper, March 2021, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

Helal, Mohamed, "The Common African Position on the Application of International Law in Cyberspace: Reflections on a Collaborative Lawmaking Process", EJIL: Talk!, 5 February 2024, https://www.ejiltalk.org/the-common-african-position-on-the-application-of-international-law-in-cyberspace-reflections-on-a-collaborative-lawmaking-process.

Hollis, Duncan, "A Brief Primer on International Law and Cyberspace", Carnegie Endowment for International Peace, 14 June 2021, https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763.

International Court of Justice (ICJ), "Corfu Channel Case", Judgment of 9 April 1949, *ICJ Reports*, 1949, https://icj-cij.org/sites/default/files/case-related/1/001-19490409-JUD-01-00-EN.pdf.

International Court of Justice (ICJ), "Costa Rica v. Nicaragua: Dispute Regarding Navigational and Related Rights", Judgment, *ICJ Reports*, 2009, https://www.icj-cij.org/sites/default/files/case-related/133/133-20090713-JUD-01-00-EN.pdf.

International Court of Justice (ICJ), "Democratic Republic of the Congo v. Uganda: Armed Activities on the Territory of the Congo", Judgment, *ICJ Reports*, 2005, https://icj-cij.org/sites/default/files/case-related/116/116-20051219-JUD-01-00-EN.pdf.

International Court of Justice (ICJ), "Legality of the Threat or Use of Nuclear Weapons", Advisory Opinion, *ICJ Reports*, 1996, https://www.icj-cij.org/sites/default/files/case-related/95/095-19960708-ADV-01-00-EN.pdf.

International Court of Justice (ICJ), "Nicaragua v. United States of America: Military and Paramilitary Activities in and against Nicaragua", Merits, Judgment, *ICJ Reports*, 1986, https://icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

International Court of Justice (ICJ), "Statute of the International Court of Justice", 1945, https://www.icj-cij.org/statute.

Irish Department of Foreign Affairs, "Position Paper on the Application of International Law in Cyberspace", 6 July 2023, https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf.

Italian Ministry of Foreign Affairs and International Cooperation, "Italian Position Paper on 'International Law and Cyberspace'", 2021, https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.

Japanese Ministry of Foreign Affairs, "Basic Position of the Government of Japan on International Law Applicable to Cyber Operations", 16 June 2021, https://www.mofa.go.jp/files/100200935.pdf.

Koh, Harold Hongju, "International Law in Cyberspace", 18 September 2012, https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf.

Lehto, Marja, "Finland's Views on International Law and Cyberspace", *Nordic Journal of International Law*, Vol. 92, No. 3 (2023), https://brill.com/view/journals/nord/92/3/article-p456_008.xml.

Moynihan, Harriet, "The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace", Journal of Cyber Policy, vol. 6, no. 3 (2021), https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1832550.

Musæus, Vibeke, "Norway's Position Paper on International Law and Cyberspace", *Nordic Journal of International Law*, Vol. 92, no. 3 (2023), https://brill.com/view/journals/nord/92/3/article-p470_009.xml.

Netherlands Government, "Appendix: International Law in Cyberspace", 26 September 2019, https://www.government.nl/binaries/government/documenten/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/international-law-in-the-cyberdomain-netherlands.pdf.

Netherlands Minister of Foreign Affairs, Letter to the Parliament on the International Legal Order in Cyberspace, 5 July 2019, https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

New Zealand Foreign Affairs & Trade, "The Application of International Law to State Activity in Cyberspace", 1 December 2020, https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf.

Ney, Paul C. Jr., General Counsel, US Department of Defense, Remarks at US Cyber Command Legal Conference, 2 March 2020, https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference.

Organization of American States, Inter-American Committee against Terrorism (OAS/CICTE), "List of Consolidated Cooperation and Confidence-Building Measures in Cyberspace", 2024.

Organization of American States (OAS), Inter-American Juridical Committee, "Improving Transparency: International Law and State Cyber Operations", Fifth Report, OEA/Ser.Q, CJI/doc. 615/20 rev.1, 7 August 2020, https://www.oas.org/en/sla/iajc/docs/CJI-doc_615-20_rev1_ENG.pdf.

Oxford Institute for Ethics, Law and Armed Conflict (ELAC), "ELAC Intervention to the United Nations Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies", 6 December 2022, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ELAC_OEWG_Intervention_-_6_December_2022.pdf.

Pakistan Mission to the United Nations, "Pakistan's Position on the Application of International Law in Cyberspace", 3 March 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf.

Polish Ministry of Foreign Affairs, "Republic of Poland's Position on the Application of International Law in Cyberspace", 29 December 2022, https://www.gov.pl/attachment/3203b18b-a83f-4b92-8da2-fa0e3b449131.

Roscini, Marco, *Cyber Operations and the Use of Force in International Law* (Oxford: OUP, 2014).

Russian Federation et al., "Updated Concept of the Convention of the United Nations on Ensuring International Information Security", Working Paper, Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies, 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.

Schöndorf, Roy, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", *International Law Studies*, 8 December 2020, https://digital-commons.usnwc.edu/ils/vol97/iss1/21.

Swedish Government Offices, "Position Paper on the Application of International Law in Cyberspace", July 2022, https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf.

Swiss Federal Department of Foreign Affairs, "Switzerland's Position Paper on the Application of International Law in Cyberspace", May 2021, https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf.

UNIDIR, Cyber Policy Portal, https://www.cyberpolicyportal.org.

United Kingdom Foreign, Commonwealth and Development Office, "Application of International Law to States' Conduct in Cyberspace: UK Statement", 3 June 2021, https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

United States Naval War College, Stockton Center for International Law, "Disruptive Technologies and International Law", 2020.

Vienna Convention on the Law of Treaties, 1969, https://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf.

Wright, Jeremy, United Kingdom Attorney-General, "Cyber and International Law in the 21st Century", 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

UNIDIR

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG