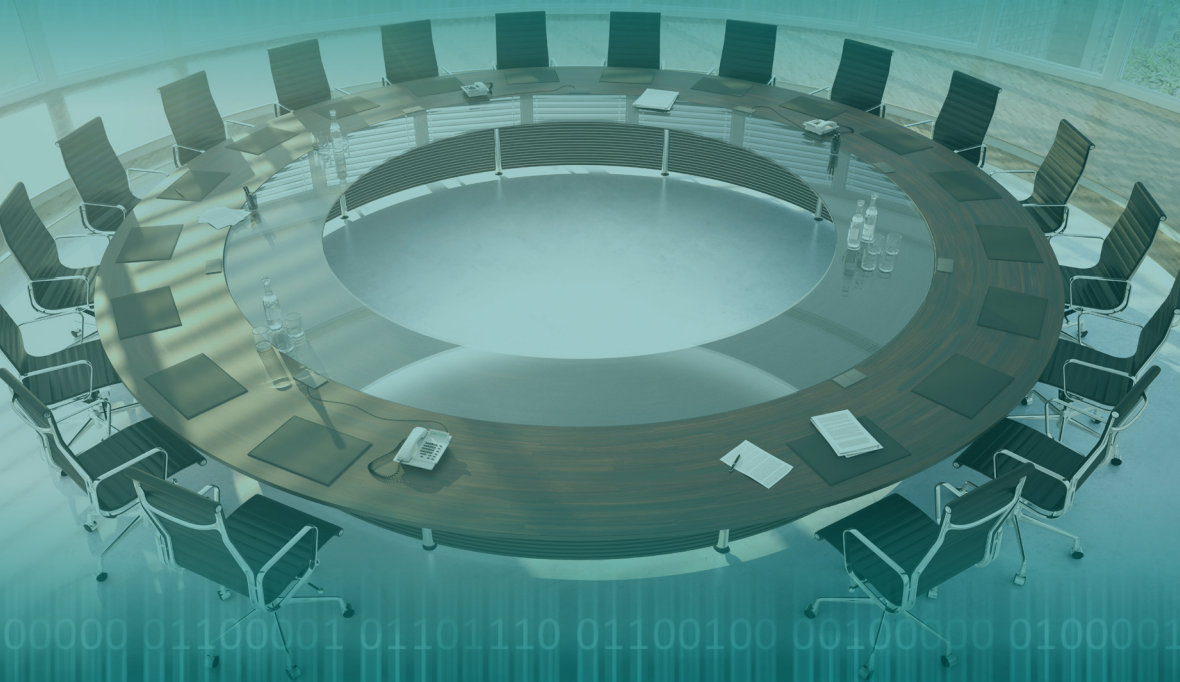


Handbook on Developing a National Position on International Law and Cyber Activities

A Practical Guide for States



Kubo Mačák, Talita Dias and Ágnes Kasper



REPUBLIC OF ESTONIA
MINISTRY OF FOREIGN AFFAIRS



MOFA
Ministry of Foreign Affairs of JAPAN



CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE



University
of Exeter



**Copyright © 2025 University of Exeter and
NATO Cooperative Cyber Defence Centre of Excellence
Professor Kubo Mačák, Dr Talita Dias and Dr Ágnes Kasper**

The right of Kubo Mačák, Talita Dias and Ágnes Kasper to be identified as the authors of this work has been asserted in accordance with the UK Copyright, Designs, and Patents Act 1988.

The digital version of this title is available Open Access and distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International licence (CC BY-NC 4.0), which permits adaptation, alteration, reproduction, and distribution for non-commercial use without further permission, provided the original work is attributed.

First published in 2025

This Handbook was developed in collaboration with the Ministry of Foreign Affairs of Estonia, the Ministry of Foreign Affairs of Japan, the NATO Cooperative Cyber Defence Centre of Excellence, and the University of Exeter.

This work was supported by an Economic and Social Research Council Impact Accelerator Account Award (grant number: ES/X004198/1; award reference: ESRC/015).

Design and layout by the University of Exeter Multimedia Design Studio

Suggested citation: Kubo Mačák, Talita Dias and Ágnes Kasper, *Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States* (2025)

Print: ISBN 978-9916-9227-0-5 PDF: ISBN 978-9916-9227-1-2 (pdf)

LEGAL NOTICE: This publication contains the views of the respective authors and it does not necessarily reflect the policy or the opinion of CCDCOE, NATO, Ministry of Foreign Affairs of Estonia, Ministry of Foreign Affairs of Japan, University of Exeter, or any other agency or government. CCDCOE, NATO, Ministry of Foreign Affairs of Estonia, Ministry of Foreign Affairs of Japan and University of Exeter may not be held responsible for any loss or harm arising from the use of information contained in this publication and are not responsible for the content of the external sources, including external websites referenced in this publication.

CONTENTS

Acknowledgements	6
List of abbreviations	8
Executive summary	10



CHAPTER 1 INTRODUCTION 12

Project	14
National and common positions	16
Legal significance of national positions	18
Structure of the Handbook	21



CHAPTER 2 MOTIVATIONS 22

Introduction	23
Overall motivations, functions, and aims	24
Specific aims and their motivations	27
Constraining factors and risks	38
Conclusion	43



CHAPTER 3 PROCESS 44

Introduction	45
National positions in the public policy and legal processes	46
Triggers	48
Stakeholders and roles	50
Preparation, planning, and start	55
Capacity-building	57
Research, analysis, and drafting	64
Adoption and dissemination	73
Follow-up, reflection, and review	73
Conclusion	74



CHAPTER 4 SUBSTANCE 76

Introduction	77
Foundational rules and principles	79
Specialized regimes	99
State responsibility	113
Conclusion	120



CHAPTER 5 PRESENTATION 124

Introduction	125
Format and style	127
Language	138
Dissemination	143
Conclusion	147



CHAPTER 6 CONCLUSION 148

What comes next?	154
Bibliography	159
Annex A: Checklist for developing a national position	168
Annex B: List of common and national positions on international law and cyber activities	170
Annex C: List of participating States	172
Annex D: List of project events	173



ACKNOWLEDGEMENTS

This project was made possible through the generous support of the United Kingdom's Economic and Social Research Council Impact Acceleration Account (ESRC IAA), whose funding enabled the development and delivery of this Handbook. We gratefully acknowledge this contribution.

We also wish to extend our sincere thanks to our institutional partners – the Ministry of Foreign Affairs of Estonia, the Ministry of Foreign Affairs of Japan, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), and the University of Exeter – for their steadfast support and collaboration throughout the project.

We are particularly grateful to Ms Karine Veersalu of CCDCOE, who served as the project manager and whose organizational skills, constant determination, and can-do attitude underpinned the smooth running of the project at all times.

We are also thankful to the staff across our institutional partners who provided essential support throughout, and whose dedication and expertise were vital to the successful execution of this project. In particular, we wish to thank Dr Anna-Maria Osula and Ms Liisa Sulavee at the Ministry of Foreign Affairs of Estonia; Mr Yukiya Hamamoto, Mr Munehito Nakatani, Mr Kimihiko Okano, Mr Satoru Onoda, and Mr Kentaro Tahara at the Ministry of Foreign Affairs of Japan; Ms Hedi Jüriöö at CCDCOE; Ms Danielle Payne and Dr James Woodhams at the University of Exeter; as well as Ms Anne Blickhan and Mr Yaroslav Halieiev who were at the time visiting scholars at CCDCOE.

We owe special thanks to our Advisory Board, whose guidance helped shape the direction of the project from the outset and whose peer review of the draft Handbook was vital to its final form. We gratefully acknowledge all members of the Advisory Board: Ms Kerry-Ann Barrett, Dr Cordula Droege, Professor Mohamed Helal, Professor Zhixiong Huang, Dr Giacomo Persi Paoli, Professor Marco Roscini, Professor Johanna Weaver, and Ms Danielle Yeow.

We warmly thank the government representatives from the 46 States who participated in the three regional roundtables. Their thoughtful engagement and openness to dialogue significantly shaped the content and focus of the Handbook. We are equally grateful to the expert briefers who enriched the discussions at each roundtable, including Ms Kristel-Amelie Aimre, Professor Mariana Salazar Alborno, Mr Benjamin Ang, Ms Larissa Schneider Calza, Mr Samit D'Cunha, Mr Yukiya Hamamoto, Professor Mamadou Hébié, Professor Mohamed Helal, Professor Zhixiong Huang, Professor Nnenna



Ifeanyi-Ajufo, Dr So Jeong Kim, Ms Eddah Mogaka, Ms Harriet Moynihan, Dr Anna-Maria Osula, Ms Kimberley Raleigh, Mr Marcus Song, Ms Liis Vihul, Ms Danielle Yeow, and Mr Robert Young. We also recognise those who formally addressed the roundtables on behalf of partner institutions, reflecting their valued support for the project, including Professor Hajer Gueldich, H.E. Mr Jens Hanefeld, Ms Irina Höhn, Professor Mart Noorma, Ms Eleliis Rattam, H.E. Mr Tanel Sepp, and H.E. Mr Priit Turk.

We also wish to acknowledge the many individuals and institutions who supported the organization of the individual roundtables.

For the roundtable on Latin American and Caribbean Perspectives, held in Washington, DC, we thank the Organization of American States for its partnership and assistance, in particular Ms Kerry-Ann Barrett and Mr David Moreno, as well as Ms Maria Tolppa of CCDCOE for note-taking.

For the Asia and the Pacific roundtable, held in Singapore, we are grateful to the Centre for International Law at the National University of Singapore, especially Ms Danielle Yeow, Ms Ying Li Loh and Ms Geraldine Ng, as well as Mr Aayush Mallik from the National University of Singapore and Ms Hanyu Zhang from Wuhan University for note-taking.

For the roundtable for African Union Member States, held in Addis Ababa, we extend our thanks to the African Union, in particular the Legal Counsel, Professor Hajer Gueldich, and to the staff of the Office of the Legal Counsel, including Mr Francis Adanlao, Ms Meseret Assefa, Ms Mitchel Mauyakufa, and Mr Taona Mwanyisa. We are also grateful to the German Federal Foreign Office and the German Agency for International Cooperation (Deutsche Gesellschaft für Internationale Zusammenarbeit, GIZ) for supporting the roundtable, especially Ms Sofia Klumpp and Ms Juliane Kolsdorf.

We gratefully acknowledge the support to all three roundtables provided by the Tallinn University of Technology through the Research Grant for Young Scientists.

Finally, we thank Dr Nicolas Bouchet for his careful review of the text and the University of Exeter Design Studio for their creative and professional work in designing and producing the Handbook.

Kubo Mačák, Talita Dias, and Ágnes Kasper
May 2025



LIST OF ABBREVIATIONS

ACHPR	African Charter on Human and Peoples' Rights
ACHR	American Convention on Human Rights
ARSIWA	Articles on Responsibility of States for Internationally Wrongful Acts
ASEAN	Association of Southeast Asian Nations
AU	African Union
CERT	Computer Emergency Response Team
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
GGE	UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
HRC	Human Rights Committee
IACtHR	Inter-American Court of Human Rights
ICC	International Criminal Court
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICJ	International Court of Justice
ICL	International Criminal Law
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technologies
ICTY	International Criminal Tribunal for the former Yugoslavia
IHL	International Humanitarian Law
IHRL	International Human Rights Law
ILC	International Law Commission



IP	Internet Protocol
NATO	
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
NATO	North Atlantic Treaty Organization
OAS	Organization of American States
OEWG	UN Open-Ended Working Group
OHCHR	Office of the United Nations High Commissioner for Human Rights
OSCE	Organization for Security and Co-operation in Europe
PCA	Permanent Court of Arbitration
SH	Stakeholder
UK	United Kingdom
UN	United Nations
UNGA	United Nations General Assembly
UNHRC	United Nations Human Rights Council
UNIDIR	United Nations Institute for Disarmament Research
UNODA	United Nations Office for Disarmament Affairs
US	United States
5W&H	Who, What, Why, When, Where, and How



EXECUTIVE SUMMARY

As States increasingly engage in cyber activities, questions about the application of international law to such conduct have gained prominence. While there is general agreement that international law applies in the cyber context, views diverge as to how specific rules and principles apply. Many States have contributed to the debate by issuing national positions: official statements outlining their legal views on key aspects of international law in the cyber context.

This Handbook provides practical guidance for States developing or reviewing their national positions, drawing on insights from 46 States that participated in regional roundtables held in Addis Ababa, Singapore, and Washington, DC in 2024, as well as on original research conducted for this project. It outlines key motivations, procedural steps, substantive legal issues, and effective presentation strategies, offering a structured approach that States can adopt at different stages of the process.

Key takeaways

- **National positions serve multiple functions:** They have a communicative function, engaging with domestic and international stakeholders; a transformative function, clarifying and adapting legal frameworks to new realities; and a preventative function, reducing the risk of misinterpretation while shaping assessments of violations and appropriate responses, thereby fostering deterrence.
- **The development process varies depending on the national context but follows common steps:** These steps include securing a mandate; assembling a core team with legal, policy, and technical expertise; conducting legal and policy analysis; consulting stakeholders and navigating interagency dynamics; determining the final format; and obtaining necessary approvals.
- **Drafting approaches can be broadly categorized as deductive or inductive:** The deductive approach begins with established rules and then analyses how they apply in the cyber context. The inductive approach starts from real-world cyber-related challenges and examines how international law applies to them. States may combine both, potentially using scenarios or case studies for clarity.



- **National positions address a wide range of substantive legal issues:** These include foundational legal principles like sovereignty, non-intervention, and the prohibition of the use of force, as well as specialized regimes such as international humanitarian law, international human rights law, and international criminal law. States should tailor the choice of topics in line with their national interests and legal priorities.
- **While there is consensus among States that international law applies in the cyber context, key differences remain:** These differences concern questions such as whether concepts like sovereignty and due diligence constitute standalone rules, how thresholds for violations should be determined, and how certain cyber activities (for example, cyber espionage) should be classified under international law.
- **The format and dissemination of national positions shape their impact:** States have issued positions as standalone papers, government speeches, and statements in multilateral forums. Clear structure, accessibility, and strategic dissemination can enhance their reach and influence.
- **National positions contribute to legal clarity in cyberspace governance:** They map areas of agreement, disagreement, and potential legal gaps. As more States issue positions, these documents will continue shaping the interpretation, implementation, and development of international law in the cyber context and beyond.
- **Future developments may include:** More detailed national positions issued by more States, greater regional coordination, adoption of new international instruments if agreement on specific gaps emerges, and domestic implementation such as integrating international legal standards into national legislation, military doctrine, and policy frameworks.

This Handbook offers a practical and structured approach for States developing or reviewing a national position, helping to foster greater legal clarity, predictability, and stability in cyberspace. By outlining existing practices, shared challenges, and strategic considerations, it offers a key resource to governments, legal practitioners, and policymakers navigating the application of international law in the cyber context.

CHAPTER 1:

INTRODUCTION



1



The rapid development of information and communication technologies (ICTs) over the past few decades has brought countless benefits to individuals and societies across the world. The emergence of cyberspace has facilitated new and more effective ways of communication, collaboration, and coordination. It has transformed economies, empowered communities, and enhanced access to information on an unprecedented scale. However, there are also significant challenges. Hostile cyber operations have caused disruption worldwide, resulting in significant human costs and affecting essential State interests. Today, it is a matter of international consensus that malicious cyber activities may have devastating security, economic, social, and humanitarian consequences that often transcend national borders.¹

As these developments unfold on a global scale, international law plays a crucial role in governing cyber activities and mitigating their impacts. Since 2013, consensus has emerged among States that international law is applicable and essential to maintaining peace, security, and stability in the ICT environment.² However, differences remain over how specific rules and principles of international law apply in the cyber context.

These discussions touch on foundational aspects of international law, such as State responsibility, sovereignty, non-intervention, and the prohibition of the use of force, as well as of specialized regimes including international humanitarian law, international human rights law, and international criminal law.

The clarification and development of the law in this area occurs to a great extent through the publication of national positions on international law and cyber activities. These official statements articulate how States interpret and apply key international legal rules and principles to cyber activities, shaping international legal discourse and influencing the development of rules and practices. As of the time of writing, 33 States have issued such positions, alongside two regional organizations – the African Union (AU) and the European Union (EU) – which have published common positions (see [Annex B](#) for a list of these documents). Several other States are considering whether to issue a national position of their own, while some with existing positions are exploring revisions or updates.

1 UN 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), para 18.

2 UN 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), para 19.



The clarification and development of international law in the cyber context occurs in large part through national positions – official statements on how States apply key legal rules to cyber activities.

This Handbook examines this growing trend, drawing on publicly available national positions, discussions in multilateral forums, and insights from closed-door consultations with State representatives. It provides practical guidance for governments seeking to develop or to review a national position, offering a structured approach to the process, content, and presentation of such documents.

Project

This Handbook is the product of a collaborative project led by a **consortium of institutions** comprising the Ministry of Foreign Affairs of Estonia, the Ministry of Foreign Affairs of Japan, the NATO Cooperative Cyber Defence Centre of Excellence, and the University of Exeter. The project has also benefitted from the support of partner institutions including the AU, the Organization of American States, the Federal Foreign Office of Germany, the Centre for International Law, National University of Singapore, and the Tallinn University of Technology.

As part of this effort, the project team organized between September and November 2024 three closed-door **regional roundtables** that brought together State representatives from the Americas (Washington, DC), Asia and the Pacific (Singapore), and Africa (Addis Ababa). These roundtables, attended by 77 officials from 46 States, provided an invaluable source of material for this Handbook. They allowed for direct exchanges between representatives of those governments that have already published national positions, those in the process of developing one, and those considering whether to do so. A full list of project events held prior to the publication of this Handbook is provided in **Annex D**.

Discussions at these roundtables were held under the **Chatham House Rule**. Accordingly, the Handbook does not attribute insights or views expressed during those meetings to specific individuals, States, or institutions, nor does it disclose their identity or affiliation. Where relevant, it does note whether a particular observation was made by a participating State representative or an invited expert, without identifying them or divulging their specific affiliation. The full list of participating States in this consultative process is included in **Annex C**.



This project builds on and complements other initiatives in this space. In particular, it draws on the *Cyber Law Toolkit* project, a leading online resource on international law and cyber operations.³ The Toolkit's comprehensive database of national positions has been an essential reference, allowing for detailed analysis of State views in this Handbook. Similarly, the *Compendium of Good Practices: Developing a National Position on the Interpretation of International Law and State Use of ICT*, published by the UN Institute for Disarmament Research in 2024, is a more concise resource that identifies best practices and procedural insights from States that have already developed national positions.⁴ The *Tallinn Manual 2.0* also served as a key reference point for the legal analysis in this Handbook, particularly with respect to the interpretation of international law in the cyber context.⁵ These initiatives have significantly contributed to the field, and this Handbook is designed to support their efforts.

³ See <https://cyberlaw.ccdcoe.org>.

⁴ UNIDIR, *A Compendium of Good Practices: Developing a National Position on the Interpretation of International Law and State Use of ICT* (2024).

⁵ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017).



National and common positions

This Handbook focusses on the development of **national positions** on the application of international law in the cyber context. One of the key takeaways from the project is the diversity of formats and approaches States have used in articulating their positions. Some have published dedicated position papers while others have expressed their views through official speeches or statements in multilateral forums. The latter were sometimes followed by the issuance of a more comprehensive document. **Chapter 5** explores these choices in greater detail as well as their legal and policy implications.

Given the range of materials available, determining which documents to include in our analysis required clear criteria. While reasonable minds may differ on what qualifies as a national position, for the purposes of this Handbook we have focussed on documents that meet all of the following conditions:

- 1. Issued publicly:** The document must be available to the general public, rather than shared only in closed-door settings such as, non-public meetings of legal advisors or closed-door sessions of the UN Groups of Governmental Experts (GGE).
- 2. Issued by a State organ:** The document must be officially issued by one or more government entities (such as a Ministry of Foreign Affairs or the Prime Minister's Office) or delivered by an official speaking on behalf of the government (such as a high-ranking diplomat or attorney general).
- 3. Available in a written format in a public repository:** The document must be published in its entirety in a format intended for long-term public accessibility, such as on a government website, in the GGE voluntary compendium, or as an official submission to the UN Open-Ended Working Group (OEWG).
- 4. Published with the aim of expressing specific legal views on the application of international law in the cyber context:** The primary purpose of the document must be to engage with substantive legal issues, rather than or at least in addition to merely reaffirming general commitments to international law or discussing matters of policy, non-binding norms of responsible State behaviour, or other non-legal questions.

A full list of documents meeting these criteria is provided in **Annex B**. For consistency, citations throughout the Handbook refer to them in the short form ‘national position of [State]’.

While the UN-based multilateral forums, such as the OEWG, focus primarily on State uses of ICTs, national positions have often gone beyond this scope, addressing the conduct of non-State actors as well. For instance, some national positions discuss whether cyber activities by non-State actors can constitute an armed attack, the obligations of non-State armed groups under international humanitarian law, and the due diligence responsibilities of States concerning cyber conduct by non-State actors within their jurisdiction. A few positions also reference cybercrime-related obligations; however, this topic has largely been addressed in separate negotiations, particularly within the UN General Assembly’s Third Committee, which led to the adoption of the UN Convention against Cybercrime at the end of 2024. Overall, the scope of national positions is broad, encompassing various issues related to the interpretation and application of international law to cyber activities.

While this project was underway, the AU and the EU each published a **common position** reflecting the shared views of their member States on the application of international law in the cyber context.⁶ These documents closely resemble national positions in structure and substance but their process differed as they were developed through consensus-building among multiple States rather than to express a single national perspective. Given their significance, this Handbook draws on and cites the AU and EU common positions throughout its analysis. In the context of the OEWG, groups of States have also occasionally issued joint cross-regional statements addressing the application of international law to the use of ICTs. However, as such common positions and joint statements involve distinct legal and political dynamics, this Handbook does not propose specific guidelines for their development. That said, much of its analysis and recommendations may be applied *mutatis mutandis* to such efforts.

⁶ Common positions of the [AU \(2024\)](#) and the [EU \(2024\)](#).



Legal significance of national positions

The status of national positions in international law remains unsettled. The positions themselves are mostly silent on this matter. Even those that discuss their broader aims typically frame them as efforts to promote legal certainty or to foster common understandings rather than make specific claims about their legal significance.⁷ Exceptionally, some positions explicitly state that their aim is to ‘develop customary law’ in general⁸ or to ‘further’ a view indicative of the emergence of a specific new rule.⁹

Discussions during the project’s roundtables were similarly inconclusive and wide-ranging. A few participants questioned whether national positions are anything more than policy documents, implying that they lack any independent legal significance. At the other end of the spectrum, others floated the idea that national positions could be considered unilateral acts giving rise to international legal obligations for the issuing State. These divergent views highlight the ongoing debate over the precise role of national positions in shaping international law and the need for further State engagement and academic research on this issue.

This Handbook does not seek to resolve this debate and instead highlights areas of common ground. Despite some scepticism, most participants in the project roundtables agreed that national positions are more than mere statements of policy. Since they are issued as official statements on the application of international law, they inherently carry some degree of legal valence, at least in relation to the sources of international law they address, including treaties and customary international law.

When national positions interpret **treaty law**, they can contribute to subsequent State practice in the application of the relevant treaty. Under the rules of treaty interpretation, if such practice establishes the agreement of the parties on a particular interpretation, it could become dispositive of the issues in question.¹⁰ However, most treaties referenced in national positions, such as the UN Charter and the Geneva Conventions, have over 150 State parties, most of whom have not yet issued such positions. Even if there is broad agreement among the States that have done so, this is insufficient to establish a definitive interpretative agreement at this stage.¹¹

7 See, for example, the national positions of Denmark (2023), p. 447, Finland (2020), p. 1, Germany (2021), pp. 1-2, Japan (2021), p. 1, Poland (2022), p. 1, Sweden (2022), p. 1, Switzerland (2021), p. 1, and the US (2021), p. 136.

8 National position of Poland (2022), p. 1.

9 National position of Estonia (2019).

10 Vienna Convention on the Law of Treaties (1969), Article 31(3)(b).

11 ILC, *Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties*, A/73/10 (2018), conclusion 10(1).



For now, the emerging shared understandings can thus only serve as supplementary means of interpretation, indicating areas where consensus may be emerging but not yet conclusive.¹²

National positions also frequently refer to rules of **customary international law**. Most commonly, States do so to affirm the customary nature of a particular rule or set of rules, such as the prohibitions of intervention¹³ and of the use of force¹⁴ or the law of State responsibility.¹⁵ On occasion, States invoke custom in the negative, rejecting the emergence of a particular rule as part of customary international law.¹⁶

Customary international law is formed through the combination of two essential elements: State practice (a general and consistent pattern of behaviour by States) and *opinio juris* (acceptance that such behaviour is

¹² Vienna Convention on the Law of Treaties (1969), Article 32.

¹³ National positions of Australia (2021), p. 2, Brazil (2021), p. 18, Costa Rica (2023), para 23, Denmark (2023), p. 449, Germany (2021), p. 4, Iran (2020), art. III 1, Italy (2021), p. 4, Norway (2021), p. 4, Switzerland (2021), p. 3, the UK (2022), and the US (2021), p. 139.

¹⁴ National positions of Brazil (2021), p. 19, Costa Rica (2023), para 35, Israel (2021), p. 398, Norway (2021), p. 5, Poland (2022), p. 5, Sweden (2022), p. 3, and the US (2021), p. 137.

¹⁵ National positions of Australia (2021), p. 5, Canada (2022), para 32, Costa Rica (2023), para 10, Estonia (2021), p. 28, Germany (2021), p. 10, Ireland (2023), para 20, Poland (2022), p. 6, Switzerland (2021), p. 5, and the US (2021), p. 141.

¹⁶ See, for example, the national positions of Israel (2021), p. 404, the UK (2021), para 12, and the US (2021), p. 141, which reject the emergence of a customary rule of due diligence.



carried out as a matter of legal obligation).¹⁷ It is fairly uncontroversial that national positions can qualify as expressions of *opinio juris*, insofar as they articulate a State's legal conviction that a certain category of conduct is permitted, required, prohibited, or even unregulated under customary international law, as the case may be.¹⁸

However, whether national positions also qualify as State practice is more contentious. Since customary international law typically develops inductively, through repeated State conduct, rather than deductively, through generalized statements, it is doubtful whether written positions alone can 'double-count' as practice and *opinio juris*.¹⁹ That said, national positions may be considered to provide evidence of State practice where they describe a State's specific cyber-related conduct, but such examples have so far been very rare.²⁰ Even if national positions (or their parts) were accepted as instances of practice, their limited number means they do not yet meet the generality requirement necessary for a new customary rule to emerge.²¹ This, however, could change as more States publish national positions.

The legal meaning of State silence in response to the publication of other States' views is unsettled. Some say States must contest interpretations they disagree with, others reject that inaction should be treated as acceptance.

A related question is whether the **silence of States** that have not issued national positions amounts to acquiescence to prevailing interpretations or to the emergence of new rules of custom.

This was a major point of discussion in the roundtables. Under international law, silence is only considered acquiescence in exceptional circumstances, with the relevant criteria including that the State in question remains silent in circumstances that require a response, that it has knowledge of those circumstances, and that a reasonable period of time has passed.²²

17 Statute of the International Court of Justice, Article 38(1)(b).

18 See also ILC, *Draft conclusions on the identification of customary international law, with commentaries*, A/73/10 (2018), conclusion 2, commentary para 4.

19 On the objection of 'double counting' more generally, see Maurice Mendelson, 'The Formation of Customary International Law', (1998) 272 *Recueil des Cours* 155, 206–207.

20 See, for example, the national position of France (2021), p. 12, which states that '[m]ost cyberoperations carried out by the French armed forces in an armed conflict situation [are] mainly information-gathering [and] do not meet the definition of attack'. See also Chapter 4, section 3.a, on the definition of attack under IHL.

21 ILC, *Draft conclusions on the identification of customary international law, with commentaries*, A/73/10 (2018), conclusion 8(1).

22 ILC, *Draft conclusions on the identification of customary international law, with commentaries*, A/73/10 (2018), conclusion 10(3); ILC, *Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties*, A/73/10 (2018), 15, conclusion 10(2).

It remains unsettled whether the publication of other States' views on international law in the cyber context creates such a circumstance. While some participants argued that States must actively contest interpretations they disagree with, others rejected the idea that inaction alone should be treated as legal acceptance. Regardless of the legal debate, there was general agreement that, as a matter of policy, it is prudent for States to respond to interpretations they consider incorrect or against their interests, lest these gradually gain wider acceptance.

Structure of the Handbook

The Handbook is divided into six chapters, following a logical progression that reflects the typical considerations and steps States go through to develop a national position. Following this introduction:

- **Chapter 2** examines the motivations behind developing a national position, exploring why States choose to articulate their views on international law and cyber activities or refrain from doing so.
- **Chapter 3** outlines the process of drafting a national position, highlighting best practices, challenges, and lessons learned from States that have undertaken this effort.
- **Chapter 4** addresses the substantive legal questions commonly covered in national positions, identifying key areas of agreement, ongoing debates, and emerging legal issues.
- **Chapter 5** provides guidance on the presentation of national positions, covering choices related to format, style, language, and dissemination.
- The **conclusion** synthesizes the key takeaways and discusses future directions for national positions in shaping international legal discourse.

In addition to the substantive chapters, the Handbook includes a practical **checklist for developing a national position (Annex A)**. This tool distills the key steps, considerations, and good practices outlined in the main text, and is designed to assist officials in planning, drafting, and delivering their national positions.

By offering a structured approach to the development, content, and presentation of national positions, this Handbook aims to support States at all stages of the process, from those considering issuing a first national position to those refining and updating an existing one. It is further intended to assist governments, practitioners, researchers, and policymakers in their work, and thus contribute to broader efforts to enhance legal clarity, predictability, and stability in cyberspace.



CHAPTER 2:

MOTIVATIONS



2

AT A GLANCE

This chapter explains why States develop national positions on international law in cyberspace. It outlines key motivations – such as promoting legal clarity, preventing miscalculation, and shaping international norms – and highlights how positions can serve both domestic and international goals. States may act to build credibility, align with partners, or respond to threats. Understanding these motivations can help guide decisions about what to include in a position and how best to use it in global legal and policy debates.

1. Introduction

Today, it is a matter of consensus that malicious cyber activities may have devastating security, economic, social, and humanitarian consequences.¹ Accordingly, steps and measures taken to prevent and respond to cyber threats or challenges, through international law or other means, are shaped by complex and often overlapping motivations. National positions are valuable legal and policy tools for addressing such threats and challenges in cyberspace. They are developed for express or implied reasons, and they may pursue external or domestic interests and aims, which may have different weight for different States. These considerations drive the decisions whether to develop a national position, which issues to address in it and to what depth, and what legal views to take on the selected substantive issues (for example, sovereignty, due diligence, and countermeasures). Factors such as the size of a State's territory, population, economy, or capabilities and other objective but context-dependent elements also shape these choices.

This chapter identifies and unpacks the motivating factors that underlie decisions about various aspects of national positions. While it is not intended to be exhaustive, the aim is to help States to pinpoint critical decision-making junctures, to understand the potential implications of different approaches, and to build persuasive arguments to support a preferred path. **Key motivating factors** can be categorized according to their external or internal dimension and in terms of the functions of national positions: communicative, transformative, and preventative. The motivations influence how the functions are deployed to achieve the **explicit or implicit aims** of a national position.

¹ UN 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), para 18.



Developing and publishing a national position is a **choice**. However, not developing or publishing one in the form of a dedicated and consolidated document, or postponing or prolonging its development does not necessarily mean that a State remains silent. States may choose to express their legal views through other venues and formats, such as oral and written contributions to the UN Open-Ended Working Group (OEWG), which may be less resource-intensive alternatives. The following sections explore the motivations and aims reflected in existing national positions and synthesize key insights drawn from the project roundtables.

2. Overall motivations, functions, and aims

a. Overall motivations

The development of a national position stems from a confluence of interconnected motivations. These statements are contextual and naturally take the perspectives of the adopting State.

Articulating their broader policy motivations can help States tailor their national position to their particular interests and formulate the specific aims they wish to pursue.

For example, while some States focus on the social or economic impact of cyber activities, and their relationship with development,² others focus on the implications of cyber activities in armed conflict.³

Although national positions have emerged in the context of international law and would typically be considered as an issue for international lawyers, many States seem to recognize that the question of how international law applies in the cyber context is (paraphrasing Georges Clemenceau) too important to be left solely to international lawyers. Articulating a national position on international law has **real-life consequences and influences** how States project power and react to projection of power in and through cyberspace. Accordingly, key drivers behind the choice of whether to develop a national position and how to formulate it arise from external as well as from internal policy considerations. Examples of external drivers include the perceived pressure to follow a group of fellow States or a push from partners and academia. These drivers are centred around the imperative to constrain States' conduct, and they define the extent of States' autonomy in and through cyberspace. However, national positions can also play significant

2 See, for example, the national positions of [China \(2021\)](#), p. 1, and [Costa Rica \(2023\)](#), paras 2-4.

3 See, for example, the national position of [Israel \(2021\)](#), p. 396.



domestic roles besides their obvious external one of addressing international legal questions. For example, developing a national position can help a State to calibrate its response to international cyber incidents, to clarify its legal obligations, and to identify domestic governance gaps that require attention.

b. Communicative, transformative, and preventative functions of national positions

National positions have a **communicative function** by engaging with relevant actors at different levels across the different elements of the broader discussion about how international law applies in the cyber context. While the topic of international law and cyberspace is not new and has been on the UN agenda since at least 1998, the trend of drafting and publicly articulating positions began about two decades later. Communicating and declaring a position on the application of international law to cyber activities to the international community and to domestic audiences signals a high level of maturity in understanding and considering the various interests involved. It also indicates that a State wants others to know what its position is, and that it has an interest in and intention to take active part in the relevant international legal processes. A national position is a way to communicate internally and externally that a State plays by the rules and expects others to do the same.

National positions have a **transformative function** by adjusting the existing framework of responsible State behaviour to new realities. Statements in national positions may have legal effects, whereby States as the primary legislators of international law contribute to the clarification, development, and evolution of the rules (see the **Introduction** on the legal valence of the positions). National positions often aspire to transform the rules of conduct in cyberspace but can significantly differ in the desired level of intensity. Developing one may thus aim at moving from grey areas to more clarity,



shaping the contours of and consolidating the existing rules, proposing a way to find common ground, or laying down the ambition to establish additional binding legal instruments in this area (which remains controversial among States). Even if the overall changes might be subtle and gradual, by clarifying the application of existing rules States begin to develop shared expectations and to define the legal boundaries of how they should behave in cyberspace. Clarification is therefore more than a merely technical exercise; it is fuelled by the perceived or real need to reshape the dynamics of international relations in the digital environment.

National positions have a **preventative function** in terms of mitigating the negative consequences of actions carried out by State and non-State actors in cyberspace, which can also serve as motivation for developing and publishing a position. By proposing an interpretation of a rule of international law, and sometimes also adding illustrative examples for more clarity, the expectation is established about circumstances when a State would consider a certain form of cyber conduct as a violation of international law and where it draws the line between legal and illegal behaviour for itself and others. Clarity about the application of rules fosters accountability for violations and serves as deterrence. Therefore, the prospect of legal consequences is a factor for ensuring restraint and respect for a State's rights.

c. Overall aims and expected outcomes

Many national positions give at least some explanation about the aims or reasons behind their publication. As these are carefully drafted texts, the explanation can focus on why a particular State decided to develop a position and also shed light on what purposes the position serves, what are the expected outcomes, and how it benefits that State and the international community. The expressly stated and the unwritten aims and expectations denote the ways in which the communicative, transformative, and preventative functions of national positions are implemented and applied. In other words, aims are the **desired outcomes and future-oriented goals** that States want to achieve by developing a national position.

These aims and expectations often overlap, reflecting the complex and multifaceted nature of the cyber domain. A few interconnected themes emerged during the project roundtables, and specific legal and/or policy aims or expected outcomes typically refer to some aspects of enhancing international peace and security, strengthening the international legal order, or consolidating the domestic environment.

3. Specific aims and their motivations

a. Preventing miscalculation and escalation – increasing predictability and stability at scale

Formulations of aims

By explicitly articulating their interpretations of international law in the cyber context, States might aim to minimize misunderstandings and to prevent unintended escalation of cyber activities, which arguably contributes to enhanced international peace and security.

This proactive approach seeks to **reduce the risk of conflict** arising from potential miscalculations or misinterpretations of actions in the digital domain. It is explicitly expressed in, for instance, the national positions of Australia, Canada, and France.⁴ As a precondition to achieve this aim, **increased trust** is also essential, as highlighted by France.

Furthermore, States may publish a position to underscore and to communicate that they are unwilling to accept a certain level of interference in their sovereign affairs. As one State representative cautioned: ‘You do not want your silence being taken for acquiescence’.⁵ Because small States are arguably more vulnerable to the kind of cyber activities in question, it is all the more important for them to make their positions known.⁶ This increased **clarity** contributes to decreasing the risk of miscalculation and misinterpretation.

A national position may also aim to increase **predictability** in State behaviour and **stability** in cyberspace. These follow from a shared understanding of how international law applies in the cyber context, and this predictability – highlighted, for example, by the national positions of Australia, Singapore, and the US⁷ – contributes to a more stable and secure international environment. The aim may be formulated as ‘promoting **responsible State behaviour** in cyberspace’, which is also expected to contribute to do so. For example, Canada states in its national position that it ‘believes that the articulation of national positions on how international law applies to State action in cyberspace will increase international dialogue and the development of common understandings and consensus on lawful and acceptable State

4 National positions of [Australia \(2021\)](#), p. 1, [Canada \(2022\)](#), para 5, [France \(2019\)](#), p. 4.

5 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

6 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

7 See, for example, the national positions of [Australia \(2021\)](#), p. 1, [Singapore \(2021\)](#), p. 85, and the [US \(2021\)](#), p. 136.



behaviour’.⁸ The national position of Australia adds that ‘[e]ven where views differ, developing understandings of respective States’ positions may increase predictability and reduce the risk of miscalculation, which can lead to escalation in State conduct’.⁹ Many States consider international law to be a fundamental element of the framework for responsible State behaviour in cyberspace.

It may be argued that these aims can be best achieved if many States express their position; hence some have encouraged adding more voices and diversity to the discussion, promoting the development of national positions and leading by example, including through participation and membership in various fora and multilateral processes.¹⁰ This may increase the **legitimacy** of these processes and their achievements.

☆ Motivations

The above aims arguably stem from the need to ensure national security, to promote economic prosperity, to improve the life of citizens, and to enhance a State’s standing in the international community. These motivations are not unique to the cyber context. To be sure, the concept of national positions is **relatively new**, and States have long managed their relations in cyberspace without them. After all, international law applies to cyber activities even in the absence of national positions. However, where uncertainty exists about how it applies, cyberspace may be perceived as a legally ambiguous or opaque domain, and misunderstandings or misinterpretations of cyber incidents could increase the risk of unintended disputes. Therefore, it is arguably more difficult to promote stability and predictability in cyberspace without clear articulations of the applicable rules of international law.¹¹ Generally, the

expression of perspectives makes it **easier to know where States stand**. In other words, a State having a national position with shared concepts and definitions¹² can enable others to understand its perspective and to act accordingly.

If a State has a national position with shared concepts and definitions, this can enable others to understand its perspective and to act accordingly.

8 See the national position of [Canada \(2022\)](#), para 5.

9 See the national position of [Australia \(2021\)](#), p. 1.

10 See, for example, the national positions of [Canada \(2022\)](#), para 6, and [Costa Rica \(2023\)](#), para 5.

11 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

12 See, for example, the national position of [Germany \(2021\)](#), p. 2.



Multiple State representatives expressed concern that voices from many regions remain **underrepresented** and that this leads to **unbalanced** discussions. The sidelining or exclusion of regions risks creating real or perceived favouritism and biases in the crystallization of how existing rules apply. This could be detrimental to effective governance, enforcement, and accountability. Hence, the argument goes that the more States speak up, the more inclusive the discussion becomes and the fewer claims can be raised later to challenge the legitimacy of UN and regional processes. Moreover, the field of cyberspace provides a unique opportunity to articulate State views, to be proactive and to keep the momentum going in efforts to uphold international peace and security.¹³

b. Enhancing compliance and accountability – deterring and preventing violations

Formulations of aims

Publishing national positions can encourage States to **adhere to their international legal obligations** and enhances **accountability** for violations. This, in turn, contributes to international peace and security as well as strengthening international legal order. National positions are also used to deter malicious actors – an objective that ranks high among States' priorities. For instance, Estonia argues that having a national position 'might also carry some deterrent effects as we have now more clarity in how we perceive and react to cyber operations in the future'.¹⁴

¹³ Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

¹⁴ National position of [Estonia](#) (2019).



In its national position, Japan states that it ‘hopes that the deepening of a shared understanding – particularly regarding which activities in cyberspace constitute a violation of international law and which tools are available under international law for States whose legal interests have been infringed by cyber operations – will deter malicious activities in cyberspace’.¹⁵ France’s national position of 2019 – one of the first issued – states that ‘[w]hile France intends to prevent, protect against, anticipate, detect, and respond to cyberattacks and do what is necessary to attribute them, it also reserves the right to respond to those which target its interests’.¹⁶ Iran also uses its national position to express intentions of deterrence in strongly worded language, including by promising ‘firmed [sic] and decisive’ consequences for violations of its ‘policies’.¹⁷ However, such formulations are the exception and the majority of national positions use a more cooperative and less confrontational tone, even when communicating red lines.

☆ Motivations

Cyber tools are an integral part of conflicts today. Therefore, every government leader will need to answer the questions about **how to act**, **how to react**, and **what are legal options** in case of violations carried out in or through cyberspace.¹⁸ Compliance and accountability are only possible if the application of rules of conduct is **sufficiently clear** and States understand where the limitations of their autonomy lay. This is also necessary for claiming potential violations of rules, as well as determining and selecting the appropriate legal responses. Furthermore, coming up with a comprehensive and consistent position is non-trivial and indicates a type of soft ‘cyber power’: the capacity to **exert influence** with regard to cyberspace.¹⁹ States might have an interest in projecting the image of having cyber power.

Furthermore, as emphasized in the national position of Australia, the effectiveness of international law hinges on States’ diligent implementation and adherence to their legal obligations as well as on collaborative efforts to uphold those obligations and to ensure accountability for breaches.²⁰

15 National position of [Japan \(2021\)](#), p. 2.

16 National position of [France \(2019\)](#), p. 5.

17 National position of [Iran \(2020\)](#).

18 Comment made at the Singapore International Cyber Week in the panel on ‘National Positions on International Law in Cyberspace: Challenges, Opportunities, and Best Practices’, 15 October 2024, Singapore (report on file with authors).

19 George Christou, ‘Cyber Diplomacy: From Concept to Practice’, *Tallinn Paper No 14*, NATO CCDCOE (2024), 5.

20 See the national position of [Australia \(2021\)](#), p. 1.

This statement emphasizes the interconnected factors that contribute to the success of international law, including clarity of rules, consistency of subjects following the rules, sharing information and calling out violations, and consequences for violations. In other words, international law cannot be effective if States only pay lip service to it.

c. Shaping the evolution of international law – addressing legal uncertainty

Formulations of aims

Statements in a national position may be very clear to emphasize that the issuing State aims to '**contribute to the discussion** on the modalities of application of international law',²¹ or that the national position is an instrument dedicated to **clarifying** the application of international law to cyber activities.²²

Other similar formulations have been used.²³ These aims may relate to the overall goal of strengthening international legal order. Another aim may be to clarify the basis for responding to unlawful acts by other States and non-State actors in cyberspace.²⁴ For example, sovereignty, the prohibition of the use of force, and the principle of non-intervention are widely believed to be the three key criteria for determining the legality of cyber operations. Most of the national positions issued so far pay a lot of attention to these three topics and the related response measures in case of violations (discussed further in **Chapter 4**).

National positions are not strictly limited to interpreting and clarifying existing rules; they can also be used to **propose new ones**, to emphasize the importance of certain rules, or to raise caution about others. For example, in their national positions, Russia and Cuba advocate the adoption of a new binding universal convention on international information security.²⁵ Therefore, it is clear that those national positions aimed to communicate a point about the State's views on how international law should develop in this area. Conversely, some States have clearly indicated that, for the time being, they see **no need for the development of a new legally binding instrument**.²⁶

21 See the national position of [Germany \(2021\)](#), p.1.

22 See the national position of [Austria \(2024\)](#), p. 3.

23 See, for example, the national positions of [Denmark \(2023\)](#), p. 447, [Estonia \(2019\)](#), the [Netherlands \(2019\)](#), p. 1, and [Switzerland \(2021\)](#), p. 2.

24 See the national position of [Denmark \(2023\)](#), p. 447.

25 See the national positions of [Cuba \(2024\)](#), para 4, and [Russia \(2021\)](#), p. 80.

26 See, for example, the national positions of [Austria \(2024\)](#), p. 3, the [Czechia \(2020\)](#), p. 2, [Estonia \(2021\)](#), p. 24, [Romania \(2021\)](#), p. 75, and [Sweden \(2022\)](#), p. 1.



Attempting to chart a middle course, others have expressed the view that these may not be mutually exclusive options. For example, the national position of Brazil states that ‘it is important to identify **convergence** amongst States on this matter and, where divergences are identified, to jointly work towards increased coherence in the interpretation of existing rules. If necessary, development of additional norms should also be considered as a means to fill potential **legal gaps** and resolve remaining uncertainties’.²⁷ Legal gaps, divergent interpretations of existing rules, and the application of different sets of rules to similar cases are not uncommon in international law. Accordingly, while convergence in legal views is a valuable goal, it does not necessarily require full uniformity. By contrast, the development of a new binding treaty would require consensus on all negotiated provisions, an objective that typically involves more extensive deliberation and agreement among States.

It emerged during the project roundtables that national positions may also aim to raise awareness about key discussions and to point out capacity-building needs on these issues. States have to consider a **complex web of interests** in their international relations. As noted by a State representative, there is a risk that support for a new legally binding instrument for cyberspace might be used as a bargaining chip in inter-State negotiations in other, unrelated matters, especially where there is little awareness of the importance of the discussions about the application of international law in the cyber context.²⁸

☆ Motivations

A key driver for issuing a national position is the desire to **actively** contribute to the international rule of law in the dynamic cyber context, as opposed to being a mere rule-taker. Sharing their views allows States to influence and to shape the interpretation and evolution of international law in the cyber context. For example, Switzerland views the national positions of States as an ‘important contribution to fleshing out the application of international law in cyberspace’.²⁹ There appears to be broad awareness and understanding of this driver, expressly in the national positions issued to date and intuitively among States aspiring to develop one.³⁰

²⁷ National position of [Brazil \(2021\)](#), p. 18. (Emphasis added.)

²⁸ Comment made at the Third Annual In-Person Symposium on Cyber & International Law, Future Conflict: The International Law of Cyber and Information Convergence in the panel on ‘Navigating Legal Dynamics: National Perspectives on International Law and Potentials for Convergence’, American University, 24 September 2024, Washington, DC (report on file with authors).

²⁹ See the national position of [Switzerland \(2021\)](#), p. 1.

³⁰ Several comments made at the project’s three roundtables (reports on file with authors).

At first glance, developing a national position might appear like an academic exercise. In reality, it is a much more **complex and consequential undertaking** concerning the core rules of international law as they relate to matters of peace and security in cyberspace. In this sense, national positions are a record of State's views on these critical issues. Therefore, there can be a significant cost to silence and non-participation in the emerging consensus on these matters. During the project roundtables, several State representatives expressed the concern that remaining silent can be (mis) construed as acquiescence to others' understandings of key legal concepts like sovereignty, non-intervention, and the prohibition of the use of force.³¹ Arguably, this risk will become more significant over time, as more States articulate their views and the international understanding of these legal concepts continues to crystallize.

Furthermore, it is not enough for States to develop their own understandings of the rules. These understandings should also be **communicated and disclosed** if they are to influence the application of existing international law or its future development in the cyber context. As the national position of Poland puts it, 'the practice of publicly presenting positions in key matters concerning international law increases the level of legal certainty and transparency, at the same time contributing to strengthening respect for international law commitments and offers an opportunity to develop customary law'.³² Reducing legal uncertainty is closely linked to upholding the rule of law, since uncertainty makes implementation and enforcement more difficult.

Recognizing the evolving nature of cyberspace, States have acknowledged the need to address and reduce legal uncertainties, identifying potential gaps in the application of international law in this context. By articulating their positions, States can contribute to filling these gaps and to **reducing the risks associated with ambiguous legal interpretations**.

Besides these considerations, **smaller States** may see the articulation of a national position as a means of **asserting and safeguarding their rights** in the international arena, where larger powers often dominate. On the other hand, larger States have a seat at the table by default, but – as noted by State representatives during the project roundtables – this comes with **responsibilities and pressure** to lead the conversation.³³

31 Comment made at the project roundtable on Africa perspectives (report on file with authors).

32 National position of Poland (2022), p. 1.

33 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).



On the other hand, there are factors that motivate States to exercise **restraint** and not to make rushed decisions announcing the need for new rules. Many States consider that, at this point in time, this area is evolving too fast and is too volatile to allow for the negotiation of an effective global treaty. It is also **unclear what the substantive content** of such a treaty could be when States have only recently begun to consider their positions and there is both convergence and divergence on key issues. Hence, these considerations also fuel formulations where States clarify what is **not their aim** or that they have no intention to take the discussions in that direction.

When **deciding** which substantive issues should be included in its national position, a State typically consider factors including the **importance** of the issue in the cyber context, its **capacity** to contribute to the clarification of the relevant issue, and the extent to which **successful domestic coordination** is likely.³⁴ In some cases, this may include a growing recognition of the need for a human-centric approach to cybersecurity that addresses the diverse needs and vulnerabilities of individuals and communities.³⁵ There is also room to present broader policy issues in national positions. Some States, like China, emphasize the need to address the digital divide and to prevent the politicization of technology and cybersecurity issues.³⁶ States with underdeveloped cyber infrastructure may be particularly interested in, for example, the international legal aspects of data embassies and more generally cloud computing,³⁷ and keep returning to the need for capacity building.

34 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

35 See the national position of [Costa Rica \(2023\)](#), para 5.

36 National position of [China \(2021\)](#), p. 1.

37 Comment made at the project roundtable on Africa perspectives (report on file with authors).

For their part, small States are naturally interested in collective responses to violations of international law.³⁸ When an interpretation or opinion is put forward that is **divergent** from others or stands out somehow (for example, Brazil considers that interception of telecommunications is a violation of sovereignty,³⁹ and Estonia furthers the view that collective countermeasures are permitted under international law⁴⁰), it is all the more important to know what are the **views of the silent majority**, as the law is evolving in this field.⁴¹

National positions have influence **beyond the cyber context** as they often engage with broader questions of general international law. There are no clearly formulated aims to this end in the national positions, but this issue was raised repeatedly during the project roundtables. This consequence of discussions about the application of international law to cyber activities is particularly visible when States articulate views on the scope, content, and elements of various primary and secondary rules of international law in general terms, prior to applying them to the specific cyber context. These expressions have the potential to influence the interpretation and understanding of the relevant rules across other areas of international law.

A clear example is the issue of sovereignty. The UK put forth the opinion in 2018 that sovereignty is a principle of international law but not a rule that can be violated as such.⁴² Many States were quick to respond, stating in their national positions that sovereignty is a standalone rule of international law and entails an independent obligation.⁴³ While the issue arose in the cyber context, the statements in national positions regarding this question are **broad** and often relate to general international law as well. Another topical issue concerns assistance from third States in the taking of countermeasures. Estonia raises the issue of collective countermeasures in its national position,⁴⁴ but now there is an **ongoing discussion** where several States have something to add.⁴⁵ Both issues are discussed in more detail in **Chapter 4** on the substance of national positions.

38 See, for example, the national positions of Costa Rica (2023), para 15, and Estonia (2019 and 2021), p. 28).

39 National position of Brazil (2021), p. 18.

40 National positions of Estonia (2019 and 2021), p. 28).

41 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

42 National position of the UK (2018).

43 See, for example, the national positions of Austria (2024), p. 4, Brazil (2021), p.18, Denmark (2023), pp. 448-449, and New Zealand (2020), para 12.

44 See the national position of Estonia (2019).

45 See, for example, the national positions of Austria (2024), p. 9, Canada (2022), para 37, Costa Rica (2023), para 15, France (2021), p. 4, and Ireland (2023), para 26.



d. Improved domestic frameworks for action and increased cyber resilience

Formulation of aims

Though domestic aims are rarely stated expressly in the national positions, it emerged from the project roundtables that many States view a clearer understanding of permissible conduct as a key expected outcome of developing such a position. This clearer understanding can serve as a framework to guide States' own cyber activities and response to cyber incidents. This framework ensures that State actions are consistent with international law, and it reduces the risk of unintended consequences.⁴⁶ The publication of a national position also gives domestic stakeholders a **point of reference** about expected behaviour.

The development of a national position can aim to increase the **cyber resilience** of the State. Having a national position contributes to enhancing resilience and preparedness to address malicious cyber operations. In this sense, national and common positions allow States to calibrate their responses since in the process they should determine, consolidate, and clarify their internal views. Moreover, working on this subject arguably improves

interagency coordination

on cyber issues by establishing lines of communication, clarifying areas of responsibility, and mobilizing key stakeholders within governments.

Though they rarely say so explicitly, many States see the development of national positions as a means of clarifying what cyber conduct is permissible.

Motivations

The development of a national position can be regarded as a **reality check**. It allows a State to better understand its readiness, to identify and to understand the interests of different domestic players, and to uncover misconceptions and misalignments. While developing a national position is a legal exercise, conversations with stakeholders shape the language, structure, and scope of the document. These conversations also enrich the legal perspectives with significant technical and policy arguments, and they can shed new light on the different implications of adopting legal interpretations. An example is whether arguing for a higher standard of due diligence is viable and realistic, and whether a State can abide by it.⁴⁷

⁴⁶ See, for example, the national position of the US (2021), p. 136.

⁴⁷ Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).



Furthermore, bringing more clarity to how international law applies in the cyber context implies **corresponding domestic action**, which may take the form of regulation.⁴⁸ Domestic stakeholders also have to consider their reality and the application of the law. As one State representative emphasized, having a national position helps ensure that various parts of the State apparatus and other actors do not engage in acts that could constitute internationally wrongful acts.⁴⁹ National positions serve as a good **reference point** for various agencies to communicate with their partners, their peers, and the general public. They centralize and align expressions relevant to State conduct in cyberspace, and stakeholders take the national position as a guidance and constraint on uncoordinated statements. Hence, the document is valuable for providing concise legal advice and for coordinating what is being communicated on cyber issues internally and externally.

When a cyber incident happens, there is often not enough time to think about how international law applies. **Cyber resilience and preparedness** require steps to be taken in advance of any incident.

By establishing a clear and coherent national stance, States can strengthen their internal legal and policy frameworks, providing a solid foundation for decision-making in the complex and often ambiguous realm of cyber operations. The digital environment is vast and various government agencies have responsibilities that cut across different aspects of cyberspace. Without dedicated attention and effort, governments may not have a full picture and may not realize where their agencies have competences and capabilities. Developing a national position is a good opportunity to **map out** how governmental networks work and what can be pulled together in case of crisis.⁵⁰ Chances are that it can also bring along domestic changes in roles, competences, procedures as well as the creation of likely scenarios for simulation exercises and working out potential response options. These are especially important to build resilience in times of crisis.⁵¹

48 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

49 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

50 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

51 Several comments made at the project's three roundtables (reports on file with authors).



Furthermore, for domestic stakeholders participating in the development of a national position, being at the table is in and of itself a capacity-building exercise. Internal considerations and the process of drafting a national position can bring domestic actors (for example, those working in defence, law enforcement, or economic affairs) in one room to jointly consider key issues. As summed up by one State representative, ‘The process itself has its value’.⁵²

4. Constraining factors and risks

While many of them articulate some of their motivations and *raison d’être*, the national and common positions published to date are typically **silent about the risks and limitations** of the exercise. Again, the reasons for this are highly contextual and differ from country to country, depending on the economic, social, and geopolitical climate and the unique traits of the domestic and external environment.

States are **free to remain silent** and to choose not to develop a national position. Having understood the importance and relevance of doing so, many are in the process of producing one, and there appear to be two main reasons why States do not (yet) have a national position: **lack of awareness and lack of capacity**.

Furthermore, as it emerged from the project roundtables, key questions also include which issues to leave out and why; how to prioritize various issues; what level of detail to aim for; how to achieve domestic agreement on divergences; whether, when and how to publicize the text; and whether and when to review an existing position.

a. Lack of capacity

Lack of capacity owing to scarce resources is a major constraint that affects decisions in the entire process of developing a national position. Doing so is a **complex and resource-intensive** undertaking. Many (or most) States lack the resources to do this or do it effectively at least in some respects. This can lead to the reprioritization of developing a national position: even if all the benefits pointed out in the previous section are understood, they might still be trumped by matters that are perceived as more urgent or important. Various issues (for example, language barriers, lack of technical or legal knowledge, prohibitive cost of participation, lack or unawareness

⁵² Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

of guidance and reference material or limitations thereof, and lack of coordination or clarity about competences within government) may make the development of a national position look like a daunting task. Hence, the decision to go ahead will inevitably be a political one. However, completely refusing to engage with the process risks granting outside influence over the interpretation of international law to other States.

Many States might also be unfamiliar or insufficiently experienced with the process of gathering State practice as an element of customary international law, which is often not publicly available. Likewise, the need for a national or common position may feel distant if a large-scale cyber incident has not yet materialized. Therefore, States would benefit from **sharing** their experiences and being transparent about their practices.⁵³

b. Absence of political will

Some government leaders may not be aware of or recognize the importance of developing a national position on international law in the cyber context. Others may lack interest in engaging with international law at all. As a consequence, some States may simply lack the political will to develop a national position. But this may come at the **cost** of not contributing to the development of State practice as an element of customary international law in the cyber context, and of not preserving leeway for being a persistent objector to the practice of others.

Caution may also be **explained** by the limited number of States having issued a national position so far, which may lead to reluctance to follow suit. Indeed, formulating a position means that careful consideration is needed from the outset, as States will normally be reluctant later to alter dramatically their published stance on such fundamental principles as the prohibition of the use of force.⁵⁴ On this basis, States may feel the need to wait until the salience of the issue increases and more clarity is achieved, maintaining flexibility for future discussions.

However, the development of national positions does not need to be a one-off exercise, and it is better viewed as part of a process, internally and externally, as part of the development of international law. Therefore, national positions are not necessarily final documents, but rather living ones, and States may decide to review them. During the project events, several

53 Comment made at workshop and project launch at CyCon, 'National Position on International Law in Cyberspace: Challenges, Opportunities and Best Practices', 28 May 2024, Tallinn (report on file with authors).

54 Comment made at the Singapore International Cyber Week in the panel on 'National Positions on International Law in Cyberspace: Challenges, Opportunities, and Best Practices', 15 October 2024, Singapore (report on file with authors).



State representatives noted that States that have published their position should study those of others and continuously review their own with the view to gradually arriving at common or shared understandings.⁵⁵ This does not necessarily mean pivoting on interpretations, but building on previous versions, and elaborating and clarifying select issues, as the understanding of relevant issues deepens and discussion matures.

c. Non-disclosure

Developing a national position does not automatically mean disclosing it immediately or rapidly. States do not have to publish their position in full or in part to reap some of the benefits of going through the process of developing it. They may choose not to prioritize publishing their views for various reasons, including:

- A desire to be agile and not be premature in positioning.
- A conservative approach of waiting for others to present their positions before disclosing one's own, and to forego unnecessary geopolitical confrontation.
- A lack or readiness to communicate certain views, leaving sensitive, controversial, or unclear issues undisclosed.
- A lack of trust and holding back from frank discussions.⁵⁶

d. Strategic omissions

The process of developing a national or common position may lead to decisions to strategically omit certain issues from the national position, to continue internal discussions on it, and to focus on issues where the State already has a solid opinion and high confidence. For example, AU member States decided not to address issues such as diplomatic immunities, the legality of countermeasures, and the conditions for invoking the plea of necessity in their common position, given disagreements on those issues.⁵⁷ States should feel **no pressure** to address all issues discussed in **Chapter 4** or to do so at once.

Moreover, States may not want to **reveal their thinking** beyond a certain level of generality, and therefore limit the depth of discussion in sensitive areas such as the threshold for qualifying conduct in cyberspace as an armed attack. In any case, States are by necessity **selective** in terms of

55 Comment made at workshop and project launch at CyCon, 'National Position on International Law in Cyberspace: Challenges, Opportunities and Best Practices', 28 May 2024, Tallinn (report on file with authors).

56 Comment made at the Third Annual In-Person Symposium on Cyber & International Law, Future Conflict: The International Law of Cyber and Information Convergence in the panel on 'Navigating Legal Dynamics: National Perspectives on International Law and Potentials for Convergence', American University 24 September 2024, Washington, DC (report on file with authors).

57 Common position of the AU (2024), para 10.



which issues they want to tackle, since they cannot cover them all.⁵⁸ What is more, if certain topics are left unaddressed, there is a risk that stakeholders can read various intentions into a State's silence or decide to interpret the text in ways unintended by its drafters. Finally, the importance of an issue for the international community in **geopolitically** difficult times may also be a determining factor in what issues to omit. In that regard, the project roundtables revealed a degree of puzzlement about the modest attention that existing national positions pay to key issues such as the peaceful settlement of disputes or the right to self-determination.⁵⁹ To respond to this need, the Handbook covers both of these in some detail in **Chapter 4**.

e. Maintaining policy and operational flexibility

States are concerned about being constrained by their public statements. Admittedly, in cyberspace, circumstances can change quickly as technology is developing at a speed that policy and law cannot keep up with. Therefore, national positions are designed not to be comprehensive or exhaustive, but as noted by a State representative during the project roundtables, help to mitigate some concerns and might need to be a *little* flexible.⁶⁰

Issuing very detailed statements can also backfire if the State cannot conduct itself in accordance with the standards it set itself, risking significant political fallout. In this sense, remaining silent can be seen as a way of avoiding accountability. Another important inhibitor is the reluctance of States to express their *opinio juris* because this may lack the flexibility to make later adjustments. This can lead to hesitation to publish anything beyond **broad and general statements**.⁶¹ While general statements can still serve a useful purpose, being overly general may be viewed as falling short of signalling a genuine commitment to playing by the rules.

Retaining constructive ambiguity and operational flexibility are key reasons why States hold back on developing a national position. Domestic stakeholders, especially the armed forces and intelligence agencies, may also see the clarification of rules as potentially constraining their activities, and as moving away from a grey area that provides them certain advantages and freedoms as well as maximum room for manoeuvring. This has the potential to **create frictions** between domestic stakeholders who might

58 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

59 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

60 Comment made at the Singapore International Cyber Week in the panel on 'National Positions on International Law in Cyberspace: Challenges, Opportunities, and Best Practices', 15 October 2024, Singapore (report on file with authors).

61 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).



differ in their approach to international relations. For example, State representatives underscored that some government agencies have a more diplomatic mindset while others are trained in and think in terms of security or military strategy. **Reconciling** these various perspectives can be a significant challenge, which needs open discussion and the willingness to compromise. It is also important to bear in mind that clarity about the rules does not only constrain but **also protects** those who observe them.⁶² For example, many States may be reluctant to accept that due diligence is a binding obligation, as it might be difficult to prevent, stop, or redress activities in cyberspace if one does not control the infrastructure.⁶³ On the other hand, precisely because of the interdependencies of cyber infrastructures there may be an appetite on the part of other States to set expectations of due diligence.⁶⁴ This logic is not dissimilar from that of due diligence in environmental law.⁶⁵

f. Lack of consensus

International law continues to evolve, and there is no clear consensus on how specific rules should be interpreted and applied in the cyber context. This can make it difficult for States to develop a coherent national position. For some, the lack of consensus may give rise to **scepticism** about such initiatives, or raise doubt about the utility of having a national or common position at all. This may also reduce the momentum or can be de-motivating for States because they are unsure about how national or common positions contribute to developing customary international law.⁶⁶

While lack of consensus can be seen as a constraining factor, it does not preclude the articulation of legal views or meaningful progress in this area. The international legal system has long functioned without universal agreement on every point of law, and **differences in legal obligations** between States – such as variations in treaty membership – **are a well-established feature** of the system. In this context, the development of national positions can help clarify legal understandings and promote convergence over time, even in the absence of full agreement.

The diversity of existing views may also prompt some States to argue for a new binding legal instrument, either to address perceived gaps or to harmonize interpretations. While this option remains open, it would, like

62 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

63 Several comments made at the project's three roundtables (reports on file with authors).

64 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

65 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

66 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

any treaty-making effort, require significant consensus among States. It is worth recalling that in other areas of international law where longstanding divergences exist, such as in the law of State responsibility, States continue to rely on customary international law rather than seek to adopt a binding multilateral treaty. This underscores the **complexity** of achieving agreement on a binding instrument and invites further reflection on the role that national positions can play in shaping legal expectations and fostering shared understandings in the cyber context.

5. Conclusion

It is important to have a clear sense of **why** a State has developed or is developing a national position. National positions have a communicative function by engaging with relevant domestic and external actors. They also have a transformative function in that they help to clarify and adjust the existing legal framework to new realities. In turn, by expressing and clarifying the position of States, national positions fulfil a preventative function as they reduce the risk of misinterpretation and miscalculation, and they help set the standard for assessing wrongfulness of conduct as well as for responses to violations, thus fostering deterrence. National positions also set aims and expected outcomes, which can be formulated in forward-looking terms. These aims and expected outcomes typically include enhancing international peace and security, strengthening the international legal order,

It is important to have a clear sense of why a State has developed or is developing a national position.

achieving clearer understanding among domestic stakeholders, and contributing to building cyber resilience.

The decision to produce a national position is **shaped by internal and**

external factors. Each position reflects the unique priorities and concerns of the State in question, often informed by the most pressing cyber threats they face. However, every State operates within its own set of circumstances – ranging from the size of its territory, population, economy, or capabilities to the degree of interagency alignment, political will, and resources availability. The choice not to develop a national position may be influenced by legal, political, or economic considerations. The project roundtables revealed two recurring reasons for this choice: a lack of capacity and a lack of political will. However, there are also factors that may limit the content or intended use of national positions, including a lack of full disclosure, the maintenance of policy and operational flexibility, or the absence of internal consensus.

This brings us to the process by which this is done, which is the topic of the following chapter.



CHAPTER 3:

PROCESS



3

AT A GLANCE

This chapter outlines practical steps for preparing a national position. It highlights the value of early co-ordination, whole-of-government engagement, and a structured drafting process. It also considers who should be involved, from legal advisers to external stakeholders, and how to navigate interagency dynamics. While each State's process will differ, clarity, inclusivity, and strategic planning are key. The chapter offers a flexible roadmap to help States craft coherent, credible, and context-appropriate national positions.

1. Introduction

The process of developing a national position varies significantly across States, with no universally applicable model to guide every case. However, certain key elements are commonly involved, even if their sequence may differ: securing a mandate, appointing penholders, conducting research into existing resources and practices, consulting stakeholders, and drafting, adopting, and disseminating the position.

Conceptually, developing a national position is rooted in the public policy cycle, but it is inherently intertwined with international law perspectives, requiring the integration of policy, legal, and operational considerations.

As a result, the process must account for all these dimensions.

Each of these steps requires resources and institutional capacity. Capacity-building remains an essential enabler for all States – particularly those with limited experience or institutional frameworks in this area – to develop and to articulate national positions on how international law applies in the cyber context.

This chapter begins by briefly exploring the dual policy and legal nature of the process before outlining the practical stages that States may go through to develop a national position. These stages include identifying what might prompt embarking on the process; determining relevant stakeholders and their roles; preparation, planning and initiation; capacity-building; conducting research, analysis and drafting; adoption and dissemination; and, finally, follow-up, reflection, and review.



2. National positions in the public policy and legal processes

The recent trend of States developing and publishing their national position on the application of international law in the cyber context reflects the **gradual evolution** of efforts to address existing and potential threats related to the use of information and communication technologies (ICTs).¹ International law is one tool – alongside confidence-building measures, technical mechanisms, and other interventions – that States employ to address cybersecurity challenges. Developing a national position is, at its core, a deliberate policy response to the cybersecurity issues a State faces.

Therefore, national positions are inherently part of the **public policy process**, as the law embodies evolving values and policy choices. Formulating a position involves addressing foreign and domestic policy concerns as well as international law considerations, as these are inextricably linked. This complexity is further compounded by the technical nature of the domain. As a result, the question of how to do it (discussed in this chapter) is often just as challenging as that of what should be included (covered in **Chapter 4**).

There is a rich body of literature and models that capture the mechanics of the public policy process.² The process is typically described in generic stages, such as problem identification and agenda, policy formulation, decision-making, implementation, and evaluation. Field-specific guidance, such as frameworks for developing national cybersecurity strategies,³ can provide valuable insights for managing the broader policy development process. These strategies often reference international law, as seen in Chile's acknowledgment that 'the challenge lies particularly on being able to identify and interpret the relevant regulations of the applicable international law'.⁴ Similarly, the EU's 2020 Cybersecurity Strategy⁵ committed the bloc to developing a common position, which was adopted in 2024. However, while such strategies may help initiate the process, they generally lack detailed guidance on the legal tasks involved, which require the expertise of legal professionals. Developing a national position necessarily draws on legal methodologies and processes unique to the legal discipline.

1 UN 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), paras 1-2.

2 For a general overview of main approaches and scholarship, see Evangelia Petridou, 'Theories of the Policy Process' (2014) 42 *Policy Studies Journal* S12.

3 *Guide to Developing a National Cybersecurity Strategy*, 2nd Edition (2021).

4 Government of Chile, *National Cybersecurity Policy*, (2017-2022), 22.

5 European Commission, *The EU's Cybersecurity Strategy for the Digital Decade* (2020), 20.



The trend of developing and publishing comprehensive national positions is relatively recent. With the repeated encouragement of the UN Open-Ended Working Group (OEWG), over 30 States have issued national positions thus far, and the number continues to grow. However, as several State representatives underscored in the context of this project, this attention might bring with it an unprecedented expectation. States may feel under pressure to present, in a single document, their whole understanding of how international law applies, which is a level of comprehensiveness rarely seen in other contexts.⁶ The complexity, coupled with these **novel expectations**, raises important questions about how to design the process of developing a national position and whether a combination of different methods would be more suited for this purpose.

These observations carry significant implications for the process of developing a national position. First, there is no universally valid protocol to guarantee success. However, certain common elements have emerged from the processes analysed in the preparation of this Handbook. Second, given the complexity and interdisciplinary nature of this exercise, States often incorporate a **mix of steps and techniques** used in public policy processes and of methodologies of international law. Third, differences in national positions indicate that the interpretations of the rules are entangled with differences in policy assumptions. This highlights the benefit of empirical methods and scenario-based discussions in the process.

The following sections explore the key elements of the process, reflecting on existing practices and challenges. However, the order in which these elements are presented do not necessarily have to be followed. Each State may tailor the process to align with its distribution of competences, administrative procedures, and institutional culture. To support State officials in navigating this effort, the Handbook also includes a concise checklist outlining key steps, considerations, and good practices for developing a national position (see **Annex A**).

⁶ Comment made at workshop and project launch at CyCon, 'National Position on International Law in Cyberspace: Challenges, Opportunities and Best Practices', 28 May 2024, Tallinn (report on file with authors).



3. Triggers

States can be prompted to start developing a national position by various factors, though, at times, it might be challenging to even bring the issue **onto the agenda**. In some cases, a significant cyberattack is a clear catalyst,⁷ with stakeholders needing little persuasion. However, painful experiences are not always necessary to raise awareness of the issue.

In many instances, participation in international discussions prompts States to develop a position, or in some cases to formalize their already formed opinions.⁸ For example, the OEWG reports have repeatedly encouraged States to share their national views on how international law applies to the use of ICTs,⁹ making the submission of such a document to the UN a tangible objective.¹⁰ After committing to the submission of a national position in an international forum, States may feel compelled to follow through in order to demonstrate leadership and to set an example.¹¹

Developing a national position may also be prompted by the need to support deterrence messaging or to clarify the legal framework surrounding offensive cyber capabilities.

For instance, Australia's 2016 Cyber Security Strategy publicly acknowledged the existence of offensive cyber capabilities and indicated that the State would use these capabilities in accordance with international law.¹² Such a declaration can trigger articulating in more detail how existing rules are understood to apply to cyber operations.

Domestic pressures can also play a role. Criticism from academics or civil society about the State's perceived inaction may push the issue up the

- 7 Comment made at the Third Annual In-Person Symposium on Cyber & International Law, Future Conflict: The International Law of Cyber and Information Convergence in the panel on 'Navigating Legal Dynamics: National Perspectives on International Law and Potentials for Convergence', American University, 24 September 2024, Washington, DC (report on file with authors).
- 8 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).
- 9 See, for example, UN General Assembly, *Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report*, A/AC.290/2021/CRP.2 (10 March 2021), para 38; UN 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), para 15; UN 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), para 33; UN General Assembly, *Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025*, A/79/214 (22 July 2024), para 40.
- 10 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).
- 11 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).
- 12 Government of Australia, *Australia's Cyber Security Strategy* (2016), 28.

policy agenda.¹³ Alternatively, States may be prompted to start the process by the need to implement a cybersecurity strategy, as seen in the case of the EU.¹⁴ Some national positions imply what prompted their development (or consolidation), and a few explicitly reference their triggers. For example, the national position of Japan notes that it ‘was prepared as a national contribution at the request of the Chair of the GGE [UN Group of Governmental Experts]’.¹⁵ The development of a national position may also be prompted by more general policies; for example, Poland’s position states that it is ‘a natural continuation of Poland’s two years of non-permanent membership of the Security Council (2018-2019), where the issue of respect for international law was one of Poland’s priorities’.¹⁶

These triggers have been important in raising awareness, in shaping the assignment of roles in the process, and in securing the mandate necessary to initiate the preliminary steps.



Figure 1: Possible triggers for the development of a national position.

13 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

14 European Commission, *The EU's Cybersecurity Strategy for the Digital Decade* (2020), 20.

15 National position of Japan (2021), p. 1.

16 National position of Poland (2022), p. 1.



4. Stakeholders and roles

As awareness grows about the importance and challenges of applying international law in the cyber context, so does the number of stakeholders involved in developing national positions. What began as a narrower discussion now includes a **wide range of voices**. Mapping stakeholders and clarifying their roles is a key step in the process. Generally, stakeholders include government agencies, consultants, civil society actors, and academics, each wielding varying levels of influence.

States should aim to assemble a multidisciplinary team that includes **legal, policy, and technical** experts. This is because the development of a national position requires a nuanced understanding of three intersecting dimensions: legal frameworks (what is permissible or prohibited), strategic implications of policy decisions (what is preferred), and the technical realities of cyberspace (what is possible). Ultimately, a well-crafted national position should balance all three.

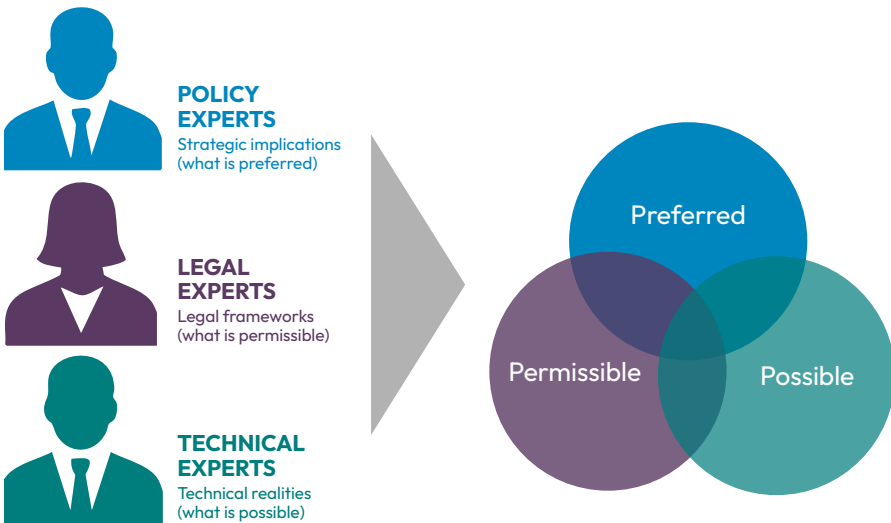


Figure 2: Composition of the drafting team.



It is important to **identify which agencies** have to be part of the process, who has the necessary authority to engage in the process and/or adopt the position, and what competences they can bring to the table.¹⁷ In some cases, this can be straightforward; for example, when legislation confers the authority to interpret international law on a specific agency. More commonly, multiple agencies have stakes in the process, including those dealing with, for example, national security, economic affairs, digital infrastructure and data, defence, foreign affairs, legal affairs, and communications.¹⁸

Some States may consider it appropriate to involve multiple agencies; for example, one with international law competences and another with technical expertise. In some cases, as one government expert put it, ‘the decision about which ones will be involved and which one will lead was made organically’.¹⁹ In other cases, this decision is made centrally and roles are assigned through formal channels. Regardless of which agency takes the lead, it is essential to raise awareness among other relevant institutions, particularly those that may not initially view the issue as a priority.²⁰ During the project roundtables, State representatives repeatedly emphasized the need for broad **political support**, since without it, the process risks stagnating or even being left incomplete.

National positions have an impact on the work and constraints of technical and operational agencies. These are the entities whose activities may qualify as State practice and who possess hands-on experience and insight into cyber operations. Accordingly, their input can significantly shape the development of national positions. Technical experts and agencies such as Computer Emergency Response Teams, Computer Security Incident Response Teams, and Security Operations Centres play a crucial role, particularly in analysing the effects of cyber operations domestically and internationally. These agencies are typically responsible for detecting, responding to, and

mitigating cyber incidents, while also engaging with international counterparts. They often hold **critical information** about cyber operations attributable to States, though such information may be technically complex,

Input from technical and operational agencies can significantly shape national positions and those positions, in turn, influence their work.

17 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

18 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

19 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

20 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).



classified, or otherwise inaccessible to legal professionals. Depending on how capabilities and competences are distributed, the same can hold true for operational agencies, like intelligence services and law-enforcement bodies, which often have **first-hand access to data about the cyber activities** of various actors, including States. This is also the case for information possessed by defence agencies and armed forces, which may possess valuable information on cyber operations. Involving all these actors in the process, at least in consultative capacity, can help ensure that national positions are informed by operational realities and reflect a coherent domestic approach, particularly on issues where legal, technical, and military considerations intersect.

One of the most influential roles in the process is that of the **penholder**. While drafting a national position is a team effort involving stakeholders within and sometimes outside the government,²¹ the appointment of a dedicated penholder or more is crucial. They will be responsible for leading the legal process, drafting the initial text, and ensuring the final product is clear, consistent, and reflective of the consensus among the parties involved.

Importantly, the penholder is not always the same as the lead agency or the political lead of the development process. If the lead agency also is the penholder, it will likely steer the substance of the conversation. However, if the two roles are separated, the lead agency will likely have political control and final decision-making authority while ensuring technical and legal input of supporting institutions. In a third model, the agency serving as the penholder may be strongly supported by international organizations or external experts in coordinating and advancing the process (in some cases, external experts have even been tasked to produce a first draft of the position).

Some roundtable participants noted that appointing the penholder(s) and/or the lead agency may lead to **competition**, and even turf wars, among institutions. In contrast, others observed that certain agencies may be **reluctant** to assume the penholder role, leading to a situation where the task 'belongs to everyone yet belongs to no one'.²² To avoid this, the choice of penholder and lead agency should be made early on in the process; and they should have strong competencies in international law and the capacity to manage the coordination, bargaining, and compromise necessary to drive the process. Likewise, the lead agency will usually have to coordinate and engage with other stakeholders involved in the process to find compromises.

21 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

22 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

When this moment arrives depends on how the process is designed and the maturity of the cyber conversation in the State.

Some national positions stand out for their structure and focus. An example is France's 2019 national position, which devotes considerable attention to international humanitarian law (IHL), more so than most other ones.²³ This likely reflects the fact that the position was produced by the Ministry of Armed Forces, and shows that the penholder and/or the lead agency possessed deep expertise in the law applicable in times of armed conflict.²⁴

Since the competences and roles related to international law often belong to them, Ministries of Foreign Affairs are often the main driver of the policy and process. However, there might not be one lead agency for international law.²⁵ In some States, **international law competences** may be in two or more agencies and the responsibilities can be shared, while in other cases there is only one agency (or none) with the necessary knowledge and expertise. Furthermore, many stakeholders involved in the process may lack legal training, let alone expertise in international law. In any case, the lead agency should be able to explain the relevance of a national position to other stakeholders, including how the decisions on the application of international law to cyber activities can affect them. However, this is a two-way street; it is just as important that the operational agencies explain what is it that they do, so the legal and policy experts have a good understanding of practice and do not get detached from reality.

The lead agency should be able to explain the relevance of a national position to other stakeholders. The operational agencies should explain what is it that they do, so the legal and policy experts have a good understanding of practice and do not get detached from reality.

23 National position of France (2019), pp. 12-16.

24 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

25 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).



Given the scarcity of relevant expertise, **informal networks** play an important role. For example, participation in GGE discussions or the Tallinn Manual consultations has helped States build capacity and enabled them to rely on these networks when drafting their position.²⁶ Therefore, creating and joining informal networks allows States to tap into a very valuable resource and address their weaknesses. However, engaging external experts and consultants may require formal agreements and face restrictions, such as security concerns or limits on external communications.²⁷

Many State representatives consulted for this Handbook emphasized the **role of public participation** in the development of national positions.²⁸ This can raise awareness, provide new insights, legitimize the end product, and increase society's receptiveness to the position. In some States, involving the public may even be a legal requirement. In other cases, this may be done on a more informal basis.²⁹ As one representative pointed out, the government's role may be limited to coordinating the positions and opinions in relevant sectors, with the Ministry of Foreign Affairs acting as a sort of spokesperson.³⁰ In such a case, inclusiveness is a very high priority.

However, inclusion can also complicate the process, potentially causing delays in finalizing the national position. It also raises the question of when to reach out to the public in order first to allow the involved agencies room for thinking and to not reveal sensitive information prematurely. While consultations are desirable in principle, they were not a consistent feature in the development of existing national positions.³¹ At a minimum, consultations should involve key stakeholders, even if the general public is not included.

Finally, the role of **policy entrepreneurs** should not be overlooked. These can be highly motivated individuals, visionaries, or dedicated academics who take up and skilfully pursue the agenda to develop a position. These persons can add significant benefit to the process in terms of leadership, subject-matter expertise and, simply put, making things happen.

26 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

27 Comment made at the project roundtable on Africa perspectives (report on file with authors).

28 Several comments made at the project's three roundtables (reports on file with authors).

29 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

30 Comment made at the project roundtable on Asia and Pacific Perspectives (report on file with authors).

31 Several comments made at the project's three roundtables (reports on file with authors).

5. Preparation, planning, and start

Preparations for the development of a national position may begin with putting the issue on the agenda or with efforts to persuade decision-makers to do so (see **Section 3** of this chapter). During the preliminary stages, roles and authority should be considered, including identifying a lead agency (see **Section 4** of this chapter). Whether this happens before, in parallel with, or after formally starting the process and assigning a mandate to the responsible agency depends on the specifics of each State.

In the **preparation and planning phase**, several key details should be clarified. These include defining what the scope of the national position will be, who will be involved and in what role, and what the process should be (that is, what steps will be taken and in what sequence, as well as what the timeline is).³² While some State representatives advocated a proactive approach (“just grab a pen and prepare an initial outline”),³³ this may not align with the bureaucratic culture in all States.³⁴

A widely used methodological tool for project preparation and planning is the 5W&H framework: **Who? What? Why? When? Where? How?** Each category prompts asking essential questions to guide the process:

Who?	Key stakeholders, including decision-makers, experts, authorities and other participants, etc.
What?	Scope, characteristics, deliverables, outcomes, events, resources, etc.
Why?	Aims, motivations, policy and legal considerations, etc.
When?	Stages, milestones, deadlines. etc.
Where?	Physical and virtual locations of resources, events, etc.
How?	Methods, processes, procedures, plans, benchmarks, monitoring, allocation of resources, etc.

32 UNIDIR, *A Compendium of Good Practices: Developing a National Position on the Interpretation of International Law and State Use of ICT* (2024), 17-18.

33 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

34 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).



At the **outset**, baselines and necessary presumptions should be established, such as that international law applies to cyber conduct and that the position will address how. It is important to have a clear ‘why’ when a national position is being developed. The scope and nature of the task (as well as of the desired outcome) should be carefully determined as this will shape institutional requirements. The interpretation of international law may fall into the exclusive competence of a certain agency, and issuing a formal statement may have to be approved by a relevant agency, like the cabinet, which may have an impact on deadlines, procedures, and other elements of the plan.

Defining the **scope** of a national position can be a difficult task at first. As discussed in **Chapter 4**, many areas of international law are relevant to ICTs. But these may be prioritized based on the State’s current needs and interests. In this context, some State representatives highlighted the importance of cross-cutting topics like the use of the internet and the impact of emerging technologies on international peace, while others flagged the issues of countering hate speech, online discrimination, and hostility and violence on social media.³⁵ Other strategies for scoping include starting with the low-hanging fruit, such as the UN Charter or other less controversial questions, before addressing more challenging issues.³⁶

Planning needs to balance **available resources**. It is important to consider how best to make use of a State’s limited resources to produce a suitable national position. These resources include time, personnel, and funding for items such as equipment, supplies, external consultants, literature, and telecommunications. Scarcity of resources can affect how relevant discussions at the national, regional, and international level will be organized, if at all. Different strategies can be used to maximize resources and creative thinking might be necessary. To address resource gaps, creative strategies might include:

- Engaging interns and volunteers.
- Involving the national academic community and industry experts.
- Applying for grants and funding opportunities.
- Collaborating with regional organizations.
- Participating in courses, roundtables, seminars, and conferences (in person or remotely).
- Leveraging freely available sources and existing international projects.

35 Comment made at the project roundtable on Africa perspectives (report on file with authors).

36 Comments made at the project roundtables on Asia and Pacific perspectives and on Latin American and Caribbean perspectives (reports on file with authors).

The length of the process for developing a national position can range from months to years, depending on the complexity of the issues and the State's capacity. However, it emerged during the project roundtables that this is not considered a one-time effort, and that positions can and should be periodically reviewed and updated to reflect new developments in domestic, regional, or multilateral policy as well as in international law and the evolving cyber environment. To ensure a timely development of the national position, detailed timelines should be set with concrete deadlines. The aim is to manage the process efficiently, including the time needed for internal and external consultations, revisions, and final approval.

6. Capacity-building

To effectively develop a national position on international law and cyber activities, it is essential to **enhance** the capabilities of all relevant stakeholders. This involves building legal and technical expertise to ensure a thorough understanding of international law and its application to ICTs. Capacity-building activities can include exercises, workshops, training programs, and conferences, and they benefit greatly from collaboration at the bilateral, regional, and international levels. These activities should adhere to the **capacity-building principles** outlined by the 2019-2021 OEWG.³⁷ These are divided into three categories concerning process and purpose, partnerships, and people.

a. Process and Purpose

- Capacity-building should be a sustainable process, comprising specific activities by and for different actors.
- Specific activities should have a clear purpose and be results-focussed, while supporting the shared objective of an open, secure, stable, accessible, and peaceful ICT environment.
- Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.
- Capacity-building should be undertaken with full respect for the principle of State sovereignty.
- Access to relevant technologies may need to be facilitated.



³⁷ UN 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), para 56.



b. Partnerships



- Capacity-building should be based on mutual trust and demand-driven, correspond to nationally identified needs and priorities, and undertaken in full recognition of national ownership. Partners must participate voluntarily.
- As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution, and monitoring and evaluation of capacity-building activities.
- The confidentiality of national policies and plans should be protected and respected by all partners.

c. People



- Capacity-building should respect human rights and fundamental freedoms, be gender-sensitive and inclusive, universal, and non-discriminatory.
- The confidentiality of sensitive information should be ensured.

Capacity-building remains a **challenge** for most States, even ones with advanced expertise, as technology develops rapidly and the discussions continue to broaden. This is not to suggest that capacity-building needs are uniform. Some States now have deep knowledge and teams of experts who are readily available for developing or revising their national position, and these States might act as donors for capacity-building. Other States might have strong capacities, such as in general international law and some specialized regimes, in which case capacity-building efforts might focus more narrowly on cyber-specific issues. In some cases, however, a comprehensive approach to capacity-building may be needed.



Importantly, the mere presence of qualified professionals does not necessarily translate into effective capacity within governmental agencies. What matters is whether the relevant expertise is available to the officials directly involved in developing the State's national position and whether they are equipped to understand and to address the associated legal and policy challenges. This becomes particularly significant given that experts and diplomats may be reassigned, rotate out of their positions, or leave public service altogether: the same pool of competencies may thus not always be **consistently available** within an agency.

Familiarization with this field often also requires some level of **technical training**.³⁸ After all, the cyber domain is a human-made environment based on engineering techniques and standards, but its impacts are broad, affecting societies and everyday life in tangible and intangible ways. Many legal questions in this field hinge on understanding the specific details of the technology.

States should actively pursue capacity-building initiatives for all stakeholders involved in developing their national position, but there is a case for prioritizing capacity-building in the lead agencies and among key stakeholders. Developing a national position and capacity-building **go hand in hand**. In fact, capacity-building is a necessary step to ensure that the position is informed, comprehensive, and aligned with the realities of the cyber domain.

The variety and success of global, regional, and national capacity-building initiatives around the world are a testament to the benefits of shared experiences and engagement with non-State stakeholders, including academia and civil society. Getting a sense of current debates in the field can help States scope out what issues they want to cover in their national position and what views they want to take on those issues.³⁹

38 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

39 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).



The OEWG has placed particular emphasis on capacity-building, which is one of the central elements of its mandate. There are **cyber capacity-building initiatives and programmes** at the UN, and recent (but general) examples are the 2024 Global Roundtable on ICT capacity building,⁴⁰ which covered a host of issues, even beyond international law and national positions, or the proposed Global Information and Communications Technologies Security Cooperation and Capacity-Building Portal.⁴¹ In 2023, the UN Secretariat conducted a mapping exercise to take stock of existing ICT security capacity-building efforts.⁴² Dozens of submissions were made by States, academia, and civil society actors, many of which listed initiatives and projects related to capacity-building on international law in the cyber context. These are available in the document database of the OEWG on security of and in the use of information and communications technologies.⁴³ Based on this mapping exercise, the UN Secretariat compiled a paper summarizing key capacity-building initiatives by thematic area of focus, including international law.⁴⁴

Examples of such initiatives dedicated to international law include:

- i. **Cyber Law Toolkit:**⁴⁵ The *Cyber Law Toolkit* is a globally accessible resource developed by a consortium that includes the Czech National Cyber and Information Security Agency, the International Committee of the Red Cross (ICRC), the NATO Cooperative Cyber Defence Centre of Excellence, the University of Exeter, the US Naval War College, and Wuhan University. Available free of charge to everyone, including government officials and legal professionals, at the time of writing the Toolkit includes:
 - a. A growing number of scenarios (currently 32) exploring the applicability of international law to cyber operations.
 - b. A database of existing national positions on the application of international law in the cyber context.
 - c. A repository of examples, which currently features over 70 cyber incidents.

40 The Global Roundtable on ICT Security Capacity-Building, held in New York on 10 May 2024, was the first event organized under United Nations auspices dedicated to the issue of capacity building. See related report: Giacomo Persi Paoli, Samuele Dominioni, Aamna Rafiq, Lenka Filipová, *Accelerating ICT Security Capacity-Building: Takeaways from the Global Roundtable on ICT Security Capacity-Building*, UNIDIR, Geneva (2024).

41 See UN General Assembly, *Initial report outlining the proposal for the development and operationalization of a dedicated Global Information and Communications Technologies Security Cooperation and Capacity-Building Portal*, A/AC.292/2025/1 (14 January 2025).

42 UN Secretariat, *ODA/2023-00042/ICT-Mapping Exercise* (2 October 2022).

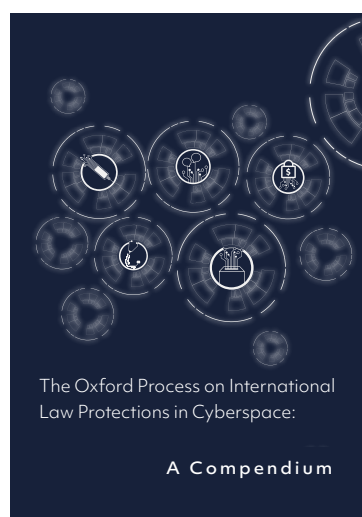
43 UNODA, Open-Ended Working Group on Information and Communication Technologies, *Documents*.

44 UN General Assembly, *Mapping exercise to survey the landscape of capacity-building programmes and initiatives within and outside the United Nations and at the global and regional levels*, A/AC.292/2024/2 (22 January 2024).

45 See <https://cyberlaw.ccdcoe.org>.

ii. The Oxford Process on International Law Protections in Cyberspace:

Launched in 2020 by the Oxford Institute for Ethics, Law and Armed Conflict in partnership with Microsoft, this initiative has produced five 'Oxford statements on international law protections in cyberspace'. These statements are the product of collaborations between international legal experts globally to clarify which conduct in cyberspace is prohibited, permitted, and required under international law in a range of contexts, including healthcare, vaccine research and development, elections, the regulation of information operations, and ransomware.





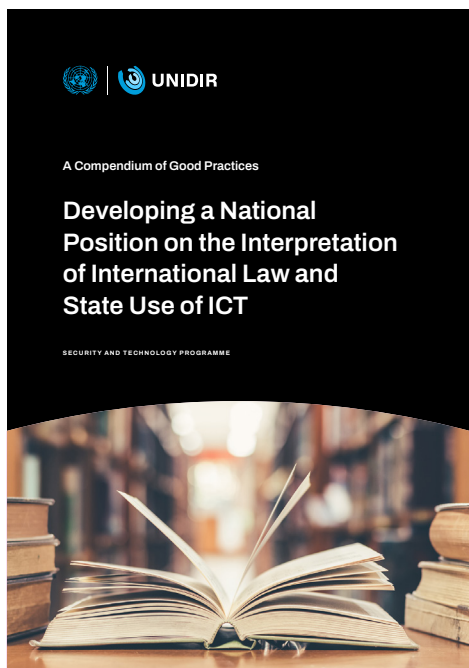
iii. **ICRC resources on IHL and cyberspace:** The ICRC provides resources and advice on the application of IHL to cyberspace for policymakers, including through bilateral dialogue, workshops, and publications.⁴⁶ The ICRC might also be able to provide advice to States on the IHL part of their national positions. Examples of further activities organized by the ICRC include humanitarian action programmes in cooperation with academia, roundtables, and other collaborative efforts.



46 ICRC, *International humanitarian law and cyber operations during armed conflicts* (2019).

Many countries and international organizations offer training and courses for officials, including the Association of Southeast Asian Nations (ASEAN), the Organization for Security and Co-operation in Europe (OSCE), and the Organization of American States (OAS). Estonia has initiated the scenario-based Tallinn Workshops on international law and cyber operations. The main objective of these thematic workshops is to create a forum for international discussions between partners and offer the opportunity to examine the most pertinent international law issues related to State conduct in cyberspace. Five workshops have been conducted and the reports of the first four have been published in a compendium.⁴⁷

In addition to the above, the 2024 *Compendium of Good Practices: Developing a National Position on the Interpretation of International Law and State Use of ICT* published by the UN Institute for Disarmament Research (UNIDIR)⁴⁸ is a concise, structured, and process-oriented resource. It offers a collection of best practices and actionable insights, making it an essential reading for those responsible for developing a national position. Many government experts consulted for this project have highlighted the compendium's practical utility.⁴⁹



47 Ministry of Foreign Affairs of Estonia, *Tallinn Workshops on International Law and Cyber Operations, Compendium of reports* (2023).

48 UNIDIR, *A Compendium of Good Practices: Developing a National Position on the Interpretation of International Law and State Use of ICT* (2024).

49 Several comments made at the project's three roundtables (reports on file with authors).



7. Research, analysis, and drafting

a. Approaches

At the initial stages of developing a national position, many States have limited experience and expertise in this field. Only a few have prior familiarity, often gained through their participation in initiatives such as the GGE and the Tallinn Manual process. As a result, the development of a national position typically involves extensive research, information-gathering, and consultations.

States generally adopt one of two approaches to structuring this process: the elimination approach or the inclusion approach.

- **Elimination approach:** This method begins with the creation of a comprehensive background research paper that identifies common topics and areas for further research. This document is then gradually refined, adapted, and reduced to produce the national position.⁵⁰
- **Inclusion approach:** This method starts with a basic rough outline that is expanded and revised as the project progresses, incorporating additional research and feedback along the way.⁵¹

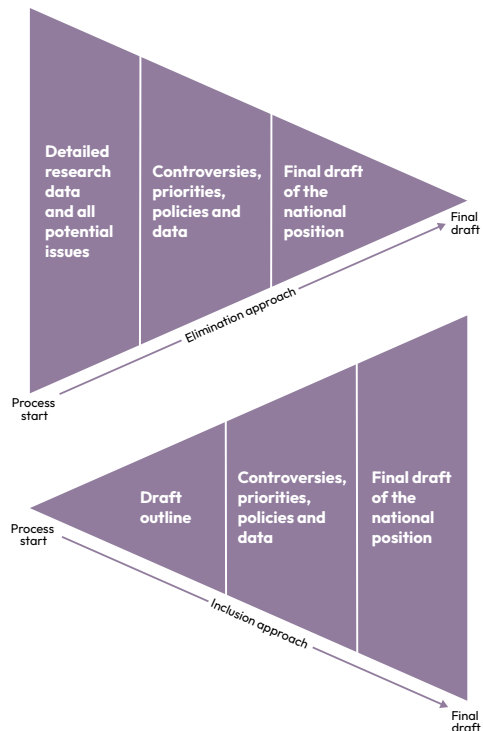


Figure 3: Two main drafting approaches.

Regardless of the approach chosen, the process typically spans months to years, and involves multiple iterations of the draft.⁵²

50 Comment at the Third Annual In-Person Symposium on Cyber & International Law, Future Conflict: The International Law of Cyber and Information Convergence in the panel on 'Navigating Legal Dynamics: National Perspectives on International Law and Potentials for Convergence', American University 24 September 2024, Washington, DC (report on file with authors).

51 Comments made at the project roundtables on Asia and Pacific perspectives and on Latin America and Caribbean perspectives (reports on file with authors).

52 Comments made at the project roundtables pointed to one to three years as the length and to at least three iterations of the draft.

b. Sources of international law and other references

Developing a national position requires extensive research to gather relevant information and to assess the associated legal and policy issues. A great deal of initial information can be collected through desk research, primarily from publicly available sources. These include legal and policy documents, reports and academic publications – cyber-specific and general. These materials are crucial for the research process and for the context of a national position, including understanding current debates and their implications, national policies, and potential priority areas.

It is important to distinguish these reference materials from the formal sources of international law defined in Article 38 of the Statute of the International Court of Justice (ICJ). While formal sources – such as treaties, customary international law, and general principles of law – are critical for the preparation of national positions, other materials provide essential background, context, and guidelines. The following diverse sources may be consulted during the drafting process:

- **National positions:** Existing national positions are a primary resource. They can be compared and analysed, and provide a basis for understanding and inspiration for selecting topics or interpretations.⁵³
- **Documents from dedicated UN fora and expert groups:** Dedicated discussions have been going on in the First Committee of the UN General Assembly, and expert groups have been studying issues of international law and cyberspace. The output by the six GGEs⁵⁴ and the two OEWGs (2019-2021⁵⁵ and 2021-2025⁵⁶) are collected and made available on the website of the UN Office of Disarmament Affairs (UNODA). These include records of government statements submitted to these groups.

53 The Cyber Law Toolkit, at <https://cyberlaw.ccdcoe.org> hosts a collection of national and common positions.

54 UNODA, Group of Governmental Experts on Developments in The Field of Information and Telecommunications in The Context of International Security.

55 UNODA, Open-Ended Working Group on Developments in The Field of Information and Telecommunications in The Context of International Security.

56 UNODA, Open-ended Working Group on Security of and in the Use of Information and Communications Technologies.



- **Other UN sources:** Various UN entities, bodies, committees, agencies, and institutions have addressed different aspects of international law that might be relevant to ICTs. These may include UN General Assembly resolutions, International Law Commission (ILC) texts,⁵⁷ UNIDIR reports and publications,⁵⁸ records of statements in the Sixth Committee of the UN General Assembly, and other specialized documents and publications.
- **Cyber-specific academic sources:** This is a very broad category and there are countless academic books and journal articles dedicated to different aspects of international law in the cyber context. Some national positions refer to specific academic sources; for example, the *Tallinn Manuals*, the *Cyber Law Toolkit* and the *Oxford Process*.⁵⁹ Publications such as the *International Review of the Red Cross*, *International Law Studies*, or the *Journal of Cyber Policy* also offer open-access articles relevant to international law and cyber activities.
- **Documents from international organizations:** Various thematic documents issued by international organizations either directly or indirectly address the issue. Examples include publications by ASEAN,⁶⁰ the AU,⁶¹ the Council of Europe,⁶² the EU,⁶³ the ICRC,⁶⁴ the OAS,⁶⁵ and the OSCE.⁶⁶
- **Primary and secondary sources of international law:** Most States use traditional sources of international law, as enshrined in Article 38 of the ICJ Statute, and expressly refer to international treaties, customary international law, general principles of law, international case law, and scholarly writings. These are vital for crafting well-substantiated and persuasive statements of the law.

57 Primarily referred to is ILC *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries* (2001).

58 UNIDIR, *Cyber security*.

59 See, for example, the national positions of *Austria* (2024), p. 3, *Costa Rica* (2023), para 6, and *Czechia* (2024), p. 1.

60 ASEAN, *Cyber security*.

61 Common position of the AU (2024).

62 On human rights and rule of law topics, including the Budapest Convention, see Council of Europe.

63 Council of the European Union, *Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace* (2024).

64 See ICRC *material on cyber and information operations*.

65 OAS, *Cybersecurity Program*.

66 OSCE, *Cyber/ICT Security*.

- **National sources:** Some States make references to domestic legislation and policies⁶⁷ as well as to declarations and strategy documents of regional organizations they are members of.⁶⁸ Furthermore, domestic case law, internal memoranda, positions expressed in international processes and many other domestic resources can be used by the drafters of a national position to clarify statements and to better understand the context, historical facts, and prior arguments. Unpublished national positions shared among close partners may also be influential and useful sources.

c. Consultations

Consultations with technical and policy experts, academia, and other stakeholders can also strengthen a national position. While the timing of consultations has varied, as a general matter, they should take place early on. But this depends on the timing of capacity-building efforts as well as on the overarching approach to the drafting process (that is, whether it follows the elimination or the inclusion approach). States have adopted one of two main consultation models:

- **Parallel routing model:** The simplest version of this model is that all the agencies or stakeholders (denoted as SH in Figures 4 to 6) start to coordinate the different views from the very beginning and carry on throughout the process. Alternatively, one or two agencies may take the lead from the beginning (marked as SH1 in Figure 5) and other agencies can be brought in for discussions once the position is developed.⁶⁹ The draft can be consolidated periodically after consultation rounds (denoted with the arrows in Figures 4 and 5).

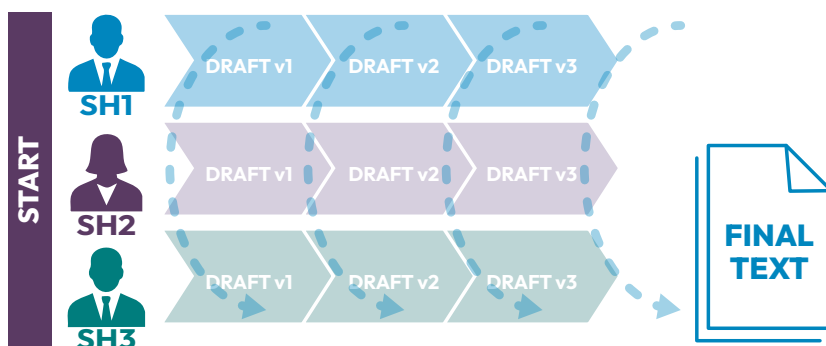


Figure 4: Parallel routing with overall coordination.

67 See, for example, the national positions of [Cuba \(2024\)](#), paras 1-2, and [Kenya \(2021\)](#) pp 53-54.

68 See, for example, the national position of [Poland \(2022\)](#) pp. 1-2.

69 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

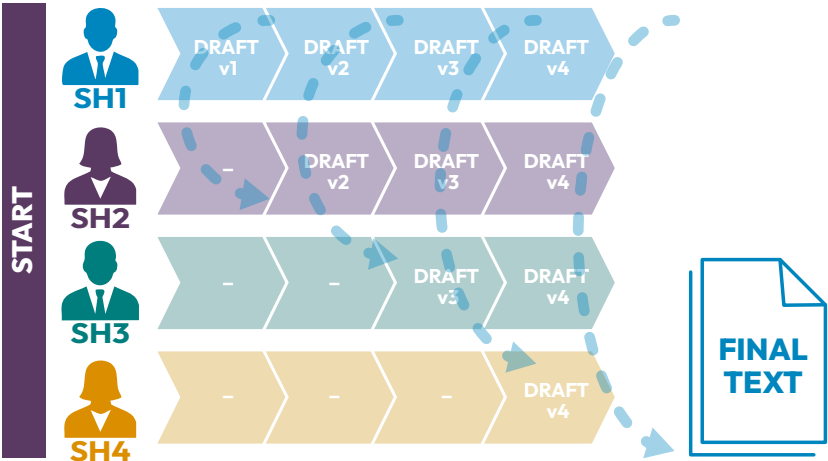


Figure 5: Parallel routing with central coordination.

Relevant stakeholders can be consulted as a single group or incrementally as the position is refined. However, incremental consultations risk creating parallel workflows, which may be time-consuming and difficult to coordinate, to de-conflict, and to consolidate. One practitioner consulted for this Handbook suggested circulating an annotated outline (rather than a full draft) for up to three comments per topic, before deciding which areas need more work.⁷⁰

70 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

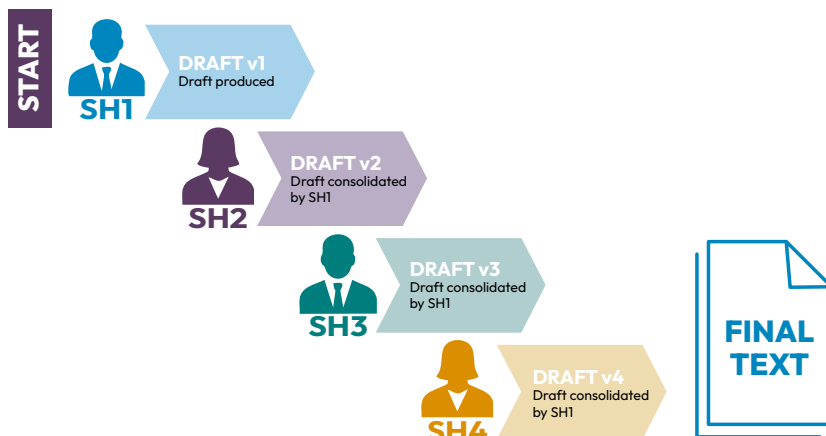


Figure 6: Continuous routing with central coordination.

- **Continuous routing model:** This approach involves conducting consultations on a rolling basis, with drafts circulated sequentially to different stakeholder groups (see Figure 6). This could mean only a one-off chance for some stakeholders to make comments and suggestions. However, this model is more streamlined and can be easier to manage.

The two models can also be combined, and the various stages can be repeated.

Consultations can be internal or external, including:

- **Interagency or departmental collaborations:** Effective interagency collaboration is important for the development of a cohesive national position and involves regular dialogue with relevant government departments. These can include national cybersecurity agencies, various ministries (for example, of defence, justice, interior, and communications), as well as the armed forces and legal organs, such as the attorney general's office or judicial bodies.⁷¹
- **Consultations with foreign government officials:** Collaboration or consultation with other States on a bilateral or multilateral basis can be useful in the different stages of the process. In particular, drafters or experts involved in the development of the national position of another State can help design and kick-off the process. Likewise, external consultations can serve as a capacity-building exercise for the State's core team and others

71 UNIDIR, *A Compendium of Good Practices: Developing a National Position on the Interpretation of International Law and State Use of ICT* (2024), 20.



involved in the process.⁷² External experts can also contribute during the drafting process, such as by giving advice on substantive or procedural matters, or by facilitating further discussions at the regional level.

- **Consultations with non-State stakeholders:** These stakeholders can be domestic or international professional associations, think tanks, consultancy firms, industry, indigenous groups, academics, or individual members of civil society (see **Section 4** in this Chapter). As noted by a State representative during the project roundtables, in States where public policy processes are very inclusive, the ‘consultation fatigue’ phenomenon should also be considered. Overall, States should seek to strike the right balance between useful input and collaboration and not overwhelming the stakeholders consulted.

Consultations may also **vary in format**. They can be formal and informal, written or oral, in-person or virtual (or hybrid), and interactive or one-way. Informal consultations can avoid extensive bureaucratic hurdles. As such, they may be easier and quicker to organize and allow for greater freedom and flexibility in the exchange of views. This can foster out-of-the-box thinking and relationship-building. However, informal consultations may not be suitable for all situations. Formal meetings may be necessary for complex issues that require detailed documentation and official records. Surveys and questionnaires can be useful in internal and external contexts, especially where different agencies are included in the discussions.⁷³ However, relevant stakeholders may lack interest or resources, or be reluctant to respond because, for example, certain issues may be deemed sensitive or classified (such as questions of attribution or IHL). Finally, town-hall or listening sessions can be especially useful in the beginning of the drafting process.⁷⁴ This may entail public meetings and essentially one-way communication between government officials tasked with developing a national position and any interested members of the public or industry. The main purpose is to collect ideas, concerns, comments, and suggestions for potential later use in the process, or identifying areas and issues where there is sufficient support to make public statements.

72 Comment at the Third Annual In-Person Symposium on Cyber & International Law, Future Conflict: The International Law of Cyber and Information Convergence in the panel on ‘Navigating Legal Dynamics: National Perspectives on International Law and Potentials for Convergence’, American University 24 September 2024, Washington, DC (report on file with authors). Also consider, for example, the series of [Tallinn Workshops](#) held by the Ministry of Foreign Affairs of Estonia.

73 Comments made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

74 Comment made at the project roundtable on Asia and Pacific perspectives (report on file with authors).

d. Analysis

Concerning the legal nature of the national positions and the process of their development, there is a vast literature dedicated to determining the **existence and content of rules**.⁷⁵ Already before the GGE's landmark conclusion in 2013 about the applicability of international law in the cyber context,⁷⁶ there was intensifying discussion about how the different rules apply. National positions are concerned with the identification of applicable rules, especially customary international law, as well as their interpretations with regard to cyber conduct. In the development of national positions, States can use deductive and inductive logics, including together (see also **Chapter 5** on format and style).

Deductive reasoning is reflected in the scoping strategy where first low-hanging issues are identified, such as the applicability of the UN Charter (see **Section 5** of this Chapter). National positions often refer to GGE and OEWG reports, which generally state the applicability of international law in the cyber context, and then the position proceeds from this general statement to the more specific rules. The deductive logic can be verified by finding examples and scenarios that confirm the accuracy of the conclusions on specific rules.

On the other hand, **inductive reasoning** is reflected in the logic that starts with identifying issues and incidents, such as ransomware or disinformation, and follows with building the position around those. As mentioned in **Chapter 5**, many States refer to scenarios in their position papers⁷⁷ and even more States promote or reportedly used scenarios in the development process.⁷⁸

⁷⁵ See, for example, the *Tallinn Manuals* 1.0 and 2.0.

⁷⁶ UN 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), para 19.

⁷⁷ See, for example, the national positions of Australia (2021), Austria (2024), Canada (2022), Costa Rica (2023), Czechia (2024), Italy (2021), the Netherlands (2019), and the UK (2022).

⁷⁸ Several comments made at the project's three roundtables (reports on file with authors).

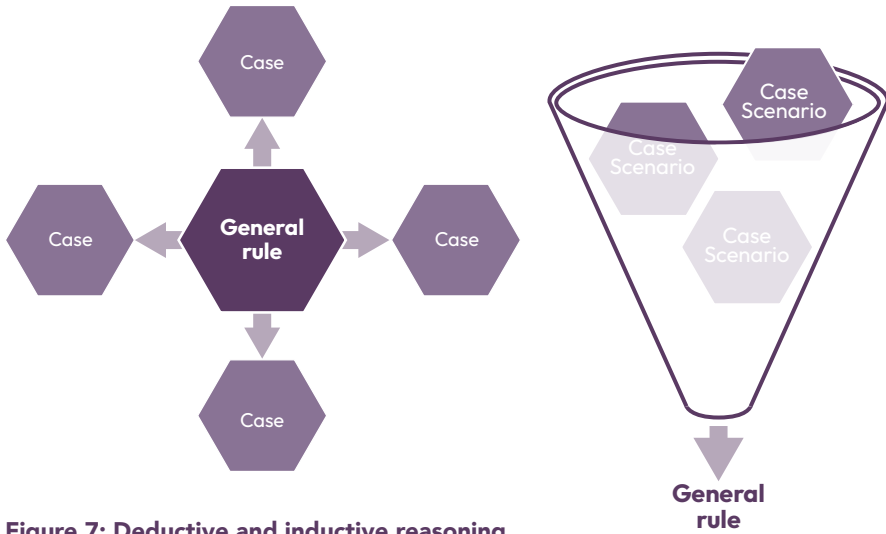


Figure 7: Deductive and inductive reasoning.

Going through different abstract formulations of a concept, and ‘playing out’ a scenario can shed light on significant practical differences in real-life application, and they make it easier to exemplify a position in the text or during consultations. However, it emerged in the project roundtables that, despite its uses, some States may be reluctant to engage in scenario-based discussions, at least in global fora. At least one governmental expert suggested that these discussions may be considered too revealing of the State’s thinking about the case. One State representative said that this reluctance may be due to infrequent uses and hence some States feeling disadvantaged.⁷⁹

Further guidance on identification of rules and interpretative tools include:

- The ILC’s Draft conclusions on identification of customary international law (2018).⁸⁰
- The ILC’s Draft conclusions on identification and legal consequences of peremptory norms of general international law (*jus cogens*) (2022).⁸¹
- The Vienna Convention on the Law of Treaties (1969).

79 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).

80 ILC, *Draft conclusions on the identification of customary international law, with commentaries*, A/73/10 (2018).

81 ILC, *Draft conclusions on identification and legal consequences of peremptory norms of general international law (jus cogens)* (2022).



8. Adoption and dissemination

The conclusion and approval of a national position requires careful deliberation to ensure that all relevant stakeholders are aligned and that it accurately represents the State's views. The State also needs to determine which internal organ(s) is (are) competent to **formally adopt or approve** the national position, in line with its domestic legal frameworks. This determination is often made during the planning phase, as discussed in **Section 5** of this Chapter.

The official adoption or approval of the national position may also need to follow a clearly defined **institutional process**. This includes designating the specific authority responsible for its endorsement. Early clarity on this matter is important. For instance, some States may require submission of the position to a legislative body for approval, while others may mandate adoption by a particular executive agency, such as a ministry or a council of ministers.

States may decide to keep a national position internal or unpublished. The national positions included in this Handbook have been made publicly available by, for instance, publishing it in an official gazette, posting on a government website, or submitting it to international forums such as the OEWG or similar platforms. As discussed in greater detail in **Chapter 5**, dissemination practices for public national positions vary and reflect the different nature and formats of these documents.

9. Follow-up, reflection, and review

After developing a national position, a State may want to consider whether further action is necessary to **implement** specific elements of the position. If implementation is required, a detailed work plan and budget should be prepared to support these efforts. Additionally, if the position sets out certain goals, mechanisms should be put in place to track and evaluate progress toward these over time.

The national positions may also be reviewed, if certain issues require **further consideration** or legal interpretations have **evolved**. This may not involve

drastic shifts in perspective but can build on previously stated views. As technology and its applications keep evolving, new issues will inevitably emerge, requiring updates to the national position.

A State may want to consider whether further action is necessary to implement specific elements of the position.



Nevertheless, revising a national position is not without challenges. A State's ability to change its position may be constrained by the need to **justify** adjustments with new circumstances, evidence, or considerations that were not taken into account previously. Sudden or significant changes in the position can carry high reputational costs, potentially undermining the State's credibility on the international stage.⁸²

10. Conclusion

The development of a national position is a **policy process and a legal one**, triggered by varying circumstances. These may range from significant cyberattacks to the fulfilment of international or domestic commitments.

A key early step is to identify relevant stakeholders and to clarify their mandates and roles. A core team should be assembled, often comprising representatives from different agencies and diverse professional backgrounds, with penholder(s) tasked with coordination and the drafting of the text. The team should include policy and technical experts alongside international lawyers, as all bring different but essential perspectives of what conduct is **preferred, permissible, and possible** in cyberspace.

The preparation and planning stages need to address various **organizational questions**, in particular who will do what, why, where, when, and how (5W&H). Capacity-building should be an integral part of the process and may be relevant in all stages. Numerous initiatives and resources are available to support States in developing the necessary expertise.

The **data-gathering, research, and analysis phase** can be approached in different ways. One method is to start with a comprehensive paper or list of issues that is then refined to narrow the scope of the national position. Alternatively, a short annotated outline can be the starting point and gradually expanded as the process evolves. **Consultations** can be an important part of the process, and they require careful coordination and management to ensure stakeholder input is effectively integrated.

82 Comment made at the project roundtable on Africa perspectives (report on file with authors).



Most national positions adopt a deductive approach, beginning with established rules of international law and then analysing how they apply in the cyber context. However, an inductive approach, starting with specific challenges (for example, AI-enabled cyberattacks or ransomware) and then examining how international law applies, can also be valuable. These **approaches can be combined**, with some States incorporating scenarios and examples to illustrate their position.

The adoption of a national position may need to follow specific **institutional requirements**, such as approval by parliament or an executive organ, depending on the State. The development of a national position is not necessarily a one-off exercise and may be subject to review.



CHAPTER 4:

SUBSTANCE

A decorative graphic consisting of several overlapping hexagons in various shades of green, brown, and orange, arranged in a honeycomb-like pattern. A large white number '4' is centered within a white-outlined hexagon on the right side of the page.

4



AT A GLANCE

This chapter surveys the main legal issues addressed in national positions, including fundamental rules and principles of international law (including sovereignty, due diligence, and non-intervention), as well as specialized legal regimes (such as international humanitarian law, international human rights law, and international criminal law). It highlights areas of agreement and key debates with a view to helping States decide which topics to cover and how deeply to engage.

1. Introduction

The existing national positions on international law and cyber activities cover a wide range of substantive issues. Alongside important questions of international law, they look at different factual aspects of the current cyber threat landscape, such as the impact of ransomware, disinformation, and cyber espionage. They have also addressed important policy challenges, such as the need to address digital divides, to foster international development, to build capacity, to address cybercrime, or to develop new rules for cyberspace. The choice of topics to cover and the views expressed on them reflect a State's stance on complex political, social, and cultural issues arising from the pervasive use of information and communications technologies (ICTs) domestically and internationally.

There is now consensus that international law is applicable to the use of ICTs, and almost all national positions to date reflect this explicitly or implicitly. The very act of publishing a position signals a State's recognition that international law is applicable and relevant to cyber activities. However, this does not mean that there is agreement on which exact rules of international law apply, how they apply in the cyber context, and whether they are sufficient to address the challenges in this context. National positions have addressed the most controversial areas of international law as they apply to cyber activities, and many areas of disagreement have become evident. Apart from the substantive debates discussed throughout this chapter, some States have argued that a new legally binding instrument is needed to fill the gaps in the application of existing international law to cyber activities.¹

¹ See, for example, the national positions of [China \(2021\)](#), p. 3, [Cuba \(2024\)](#), para 4, [Pakistan \(2023\)](#), para 8, and [Russia \(2021\)](#), p. 80.



This chapter is structured around three broad categories of legal issues that arise in the application of international law to cyber activities. It begins with an examination of foundational rules and principles of international law, including sovereignty, non-intervention, the prohibition of the use of force, due diligence, peaceful settlement of disputes, and self-determination. It then turns to three specialized legal regimes – international humanitarian law, international human rights law, and international criminal law – and examines how their rules apply in the cyber context. Finally, it analyses the law of State responsibility, focussing on attribution, countermeasures, and the plea of necessity.

These discussions are vital in determining how existing legal frameworks can adapt to the unique challenges posed by ICTs. And national positions have become the primary vehicle through which States have contributed to those important legal debates. As noted in the **Introduction** to this Handbook, national positions may qualify as evidence of *opinio juris* and, more controversially, of State practice for the purposes of the formation of customary international law. Accordingly, it is open to States to maintain the status quo or to develop international law through their national positions.

This chapter provides an overview of the most frequent substantive international law issues featured in the national and common positions published to date (see also Figure 8 on pages 122 and 123), as well as in relevant multilateral discussions, including in the context of the UN-mandated processes such as the UN Group of Governmental Experts (GGE) and the UN Open-Ended Working Group (OEWG). The selection of topics also reflects those consistently raised by participants in the project roundtables. In addition to mapping the different views of how these rules and principles of international law apply in the cyber context, the chapter also examines the policy considerations that shape them.

To assist readers in exploring these topics in greater depth, this chapter includes QR codes – which are clickable in the digital version – that link to the corresponding pages of the *Cyber Law Toolkit*. These pages provide regularly updated content, further legal analysis, and a comparative overview of national positions on each issue.

2. Foundational rules and principles

This section examines six foundational rules and principles of international law as they apply to cyber activities. Four of them – sovereignty, the prohibition of intervention, the prohibition of the use of force, and due diligence – feature in a significant number of national positions and are among the most frequently discussed topics in this area. The other two – peaceful settlement of disputes and the right to self-determination – have attracted less attention but are beginning to appear more regularly in national positions and multilateral discussions. While most would agree that all six apply to cyber activities, States differ in how they interpret and apply them. Overall, this section outlines how States that have published a position to date have approached these issues, highlighting areas of convergence and unresolved questions.



a. Sovereignty

Sovereignty is a core principle of international law. According to a classic definition, articulated in the 1928 *Island of Palmas*² arbitral award, sovereignty signifies, ‘in regard to a portion of the globe [...] the right to exercise therein, to the exclusion of any other State, the functions of a State’. It is generally accepted that sovereignty applies in the cyber context.³ However, debate persists regarding its precise legal nature: does it constitute a standalone rule of international law or

does it operate merely as a guiding principle?

There is broad consensus that sovereignty applies in the cyber context, though debate remains on whether it is a standalone rule of international law or merely a guiding principle.

² *Island of Palmas (US v Netherlands)* (1928) II RIAA 829, 838.

³ UN 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), paras 70, 71(b).



Most States that have expressed a position on this matter consider sovereignty to be a **substantive primary rule of international law**, the breach of which gives rise to State responsibility. Importantly, this may trigger the right of the victim State to take countermeasures against the State responsible for the violation. This view has been adopted by States including Austria, Brazil, Canada, Czechia, Estonia, Finland, France, Germany, Iran, Italy, Japan, the Netherlands, New Zealand, Norway, Romania, and Sweden.⁴ It has also been endorsed in the common position of the African Union (AU) and the common position of the European Union (EU).⁵

There is also the view that sovereignty is merely a **principle of international law** that guides State interactions but does not amount to a standalone primary rule. This position has been adopted by one State so far, the UK. Under this approach, cyber operations cannot violate the sovereignty of the State into or against which they are directed. However, such operations may still constitute prohibited intervention, uses of force, or other internationally wrongful acts.

A **middle approach** simply acknowledges that sovereignty applies in the cyber context while refraining from clarifying whether it constitutes a rule of international law. Some States adopting this position further note the complexity of the issue and indicate that they are continuing to study it. This approach allows States to preserve operational flexibility and retain the option of endorsing a more definitive position in the future. States that have taken this stance include Australia, Israel, Kenya, and the US.⁶

The prevailing view that sovereignty constitutes a standalone rule implies an obligation on all States to respect the sovereignty of other States. However, there is at present no consensus on the exact criteria for determining when cyber operations violate sovereignty, and State positions vary significantly. Two main approaches have emerged in this regard: the access-based approach and the effects-based approach.

4 See the national positions of Austria (2024), p. 4, Brazil (2021), p. 18; Canada (2022) paras 10 and 14 ff, Czechia (2024), paras 1 and 3, Estonia (2021), p. 24, Finland (2020), pp. 1-2, France (2021), pp. 2-3, Germany (2021), pp. 2-3, Iran (2020), art. II.2, Italy (2021), p. 4, Japan (2021), p. 2, the Netherlands (2021), p. 7, New Zealand (2020), paras 11-15, Norway (2021), p. 3, Romania (2021), p. 76, and Sweden (2022), p. 2.

5 See the common positions of the AU (2024), para 12 and the EU (2024), p. 4.

6 See the national positions of Australia (2021), p. 5; Israel (2021), p. 402; Kenya (2021), p. 53, and the US (2021), p. 139.



- According to the **access-based approach** (also referred to as the penetration-based or purist approach), any unauthorized penetration of ICT systems located within the territory of a State qualifies as a violation of that State's sovereignty. This includes operations such as installing a backdoor in an ICT system or exfiltrating data from such a system. States in favour of this approach may choose to endorse it for its protective qualities.⁷ However, those against it highlight its potential incompatibility with the design and operation of the internet, particularly the fact that any online communication, by definition, involves entering the recipient's network.⁸
- The **effects-based approach** requires a cyber operation to produce some kind of effect on or harm to the victim State to qualify as a violation of sovereignty. The possible proscribed effects or harms as identified in the literature include infringement of the territorial integrity of the victim State and interference with or usurpation of the victim State's inherently governmental functions.⁹
 - An operation can **infringe a State's territorial integrity** in several ways. The most obvious is by causing physical damage, destruction, injury, or death. Acts having such effects may simultaneously qualify as violations of non-intervention and as uses of force (see below). In their national positions, some States extend this category to include the loss of functionality of systems located in another State, even if such loss does not result in physical damage.¹⁰
 - The notion of **inherently governmental functions** covers activities that are exclusively within the competence of a State and can only be exercised by non-State actors upon State delegation, such as national defence, law enforcement, provision of social services, organizing elections, or conducting diplomacy.¹¹ *Interference* with such activities involves disrupting them, such as manipulating election results through cyber means. *Usurpation* occurs when a cyber operation involves carrying out a function that only the affected State is authorized to perform, such as exercising law enforcement powers in another State's territory without its consent.

7 Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* (Chatham House 2019), para 61, describing this approach as 'maximally protective'.

8 See, for example, the national position of the US (2021), p. 140, which states that '[t]he very design of the Internet may lead to some encroachment on other sovereign jurisdictions.'

9 Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) (*Tallinn Manual 2.0*), commentary to Rule 4.

10 See, for example, the national positions of Austria (2024), p. 4, Canada (2022), paras 16-17, Costa Rica (2023), para 20, Denmark (2023), p. 449, and Norway (2021), pp. 3-4.

11 *Tallinn Manual 2.0*, commentary to Rule 4.



An unsettled question concerns **cyber espionage**. While international law does not regulate it as such, espionage's lawfulness may be difficult to reconcile with the broader views on sovereignty outlined above, particularly the access-based approach. If any unauthorized data collection abroad constitutes a violation of sovereignty, this would encompass many cyber espionage operations. In their national positions, States including Austria, Costa Rica, and Poland expressed views suggesting that they consider at least certain types of cyber espionage to violate sovereignty. In Brazil's position, interceptions of telecommunications are by definition unlawful because they violate State sovereignty.¹²

By contrast, some States expressly take the opposite view in their national positions. For example, Canada's states that 'some cyber activities, such as cyber espionage, do not amount to a breach of territorial sovereignty',¹³ while New Zealand's notes that it 'does not consider that territorial sovereignty prohibits every unauthorised intrusion into a foreign ICT system' and that 'pure espionage activity [...] would not be internationally wrongful'.¹⁴ Ultimately, the qualification of cyber espionage remains unsettled and is likely to continue shaping States' positions on sovereignty in cyberspace.



b. Non-intervention

The principle of non-intervention (also referred to as the prohibition of intervention) is a corollary of State sovereignty and a well-established rule of customary international law. It prohibits States from interfering, directly or indirectly, in the internal or external affairs of other States by coercive means.¹⁵ There is no question that the principle of non-intervention applies in the cyber context. For an act, including a cyber operation, to qualify as a prohibited intervention, it must fulfil two

key conditions.

First, it must bear on **matters within a State's internal or external affairs** – its **domaine réservé**: in other words, those issues on which each State is permitted to decide freely, such as the choice of its political, economic, social, and cultural systems, as well as the formulation of its foreign policy.¹⁶

¹² National position of [Brazil \(2021\)](#), p. 18.

¹³ National position of [Canada \(2022\)](#), para 19.

¹⁴ National position of [New Zealand \(2020\)](#), para 14.

¹⁵ ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US)* (Merits) [1986] ICJ Rep 14 (*Nicaragua Case*), para 205.

¹⁶ ICJ, *Nicaragua Case*, para 205. See also ICJ, *Case Concerning Armed Activities in the Territory of the Congo (Democratic Republic of Congo v Uganda)* (Merits) [2005] ICJ Rep 168, paras 162–64; [Tallinn Manual 2.0](#), commentary to Rule 66, paras 6–8.



For some, the content of the *domaine réservé* is limited by the scope and nature of a State's international legal obligations.¹⁷ On this view, the more international rules a State has agreed to, the less freedom it has over its internal or external affairs and the narrower the scope of its *domaine réservé*. For others, the scope of a State's *domaine réservé* is fixed and corresponds to a standard list of inherently sovereign functions.¹⁸

In the cyber as well as in other contexts, adopting the former approach would limit the areas in which intervention is considered unlawful and therefore reduce the scope and import of the non-intervention principle. For example, if a State has agreed to certain international health standards, interference with regard to these standards by cyber or non-cyber means would not be considered a prohibited intervention. In contrast, a fixed approach to *domaine réservé* would result in a wider scope of application for the principle of non-intervention. Using the same example as above, the fact that a State has agreed to a certain international obligation in the context of healthcare would not entirely remove its freedom on the matter. After all, States still retain discretion and ultimate authority in matters over which they exercise governmental authority.¹⁹

Most national and common positions issued so far have taken the latter approach and not limited the areas falling within a State's *domaine réservé*.²⁰ This 'protective' approach seems to stem from a concern to limit intrusive cyber operations carried out or supported by other States. The opposite view seems to be connected to 'expansive' cyber strategies that seek to preserve a State's ability to carry out cyber activity abroad.²¹

17 See, for example, *Tallinn Manual 2.0*, commentary to Rule 66, paras 7 and 13; Katja S Ziegler, 'Domaine réservé' (April 2013), *Max Planck Encyclopedia of International Law*, Section C; Marco Roscini, *International Law and the Principle of Non-Intervention* (OUP 2024) 162–164.

18 See, for example, Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* (Chatham House 2019), para 107. See also the discussion in Tsvetelina van Benthem, Talita Dias, and Duncan B Hollis, 'Information Operations under International Law' (2022) 55 *Vanderbilt Journal of Transnational Law* 1217, 1260–1261.

19 Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* (Chatham House 2019), para 106.

20 See, for example, the national positions of Costa Rica (2023), paras 23–25, Czechia (2024), para 9(a), Denmark (2023), p. 450, and Ireland (2023), paras 8–10, which all list non-exhaustive areas within a State's *domaine réservé*, and also the national position of Canada (2022), para 22, which defines the scope of non-intervention around 'inherently sovereign functions'.

21 See, for example, the national position of the US (2021), p. 140, which argues that non-intervention 'is generally viewed as a relatively narrow rule of customary international law'.



Coercion is the second element of a prohibited intervention: the act in question must be **coercive in nature**. According to the International Court of Justice (ICJ), '[t]he element of coercion[[...] defines, and indeed forms the very essence of, prohibited intervention'.²² Coercion may be direct, exerted by the organs of one State against those of another, or indirect, in the form of support for the coercive acts of non-State actors or acts targeting the population of the victim State (as opposed to its government).²³ An example of direct intervention is military action in the territory of another State. Examples of indirect intervention include State support for the subversive actions of non-State actors or influence operations seeking to change the attitudes of the victim State's population, such as certain forms of propaganda and disinformation. Indirect intervention is particularly pronounced in the cyber context given the proliferation of ICTs among non-State actors, including as perpetrators or victims of malicious cyber operations.

Coercion is a key element of a prohibited intervention: the act in question must be coercive in nature.

However, there is no generally accepted definition of coercion in international law.²⁴ There are two main approaches to defining coercion in the cyber context, focussing on two different elements:

- a. The **intent-based** approach, under which an act is coercive if it is designed to compel the victim State to change its behaviour with respect to a matter within its *domaine réservé*.²⁵
- b. The **effects-based** approach, under which coercion means actual deprivation of control; that is, to be coercive, the act must effectively deprive the victim State of its ability to control or govern matters within its *domaine réservé*.²⁶

²² ICJ, *Nicaragua Case*, para 205.

²³ ICJ, *Nicaragua Case*, para 205; UN General Assembly, *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States*, A/RES/36/103 (9 December 1981), Annex, Part II, letters f, g, j, l, m and n.

²⁴ Mohamed Helal, 'On Coercion in International Law' (2019) 52(1) *NYU Journal of International Law and Politics* 1, 3. See also Marco Roscini, *International Law and the Principle of Non-Intervention* (OUP 2024), 147–158.

²⁵ See, for example, the national positions of Austria (2024), pp. 5-6, Canada (2022), para 22, Czechia (2024), paras 9-11, Estonia (2021), p. 25, Germany (2021), p. 5, Italy (2021), pp. 4-5, the Netherlands (2019), p. 3, Norway (2021), p. 4, and Switzerland (2021), p. 3. This was also the view endorsed by the majority of the *Tallinn Manual 2.0 Experts*: see *Tallinn Manual 2.0*, commentary to Rule 66, para 19.

²⁶ See, for example, the national positions of Australia (2021), p. 3, New Zealand (2020), paras 9-10, and the UK (2022).

Each approach leads to different results and is grounded in different policy considerations. For example, in a case involving electoral interference, which most States agree could amount to prohibited intervention,²⁷ the *intent-based approach* would require proof that the cyber operation in question was intended to influence a State's electoral process. Proof of intent might be difficult to produce, especially in the cyber context, which is marked by secrecy. Yet this requirement ensures that State policies or actions that have unintended consequences abroad are not considered prohibited interventions.

Conversely, the *effects-based approach* would require proof that the cyber operation in question produced concrete results that actually affected a State's ability to carry out an election, such as disabling voting machines or dissuading voters. The downside to this approach is that proof of a causal link between certain types of cyber operations, such as influence operations, and the actual deprivation of a State's ability to control its internal or external affairs, might be difficult to produce. This approach seems to be motivated by the need to prevent and sanction harmful intervention, despite the difficulty in obtaining proof of a coercive intent.

There are variations on these approaches too. For example, the common position of the AU endorses a broader version of the intent-based approach whereby coercion is 'a policy [...] designed to impose restraints on the will of a foreign State'.²⁸ Accordingly, in the view of the AU, coercive effects are not necessary for a violation of non-intervention to occur; provided that a policy to impose restraints is present, threats or unsuccessful attempts to interfere could constitute a prohibited intervention.²⁹ Costa Rica takes an even broader view, stating that 'it suffices that a State intends to coerce another State, employs coercive methods, or eventually causes coercive effects in another State' for the principle of non-intervention to be breached.³⁰ On this view, coercion might be demonstrated by different means – namely the presence of a coercive intent, coercive effects, or the use of coercive methods that have the potential to deprive a State's ability to control or choose how to govern its internal or external affairs – irrespective of the intent or effects caused.³¹

27 See, for example, the national positions of Australia (2021), p. 3, Brazil (2021), p. 19, Canada (2022), para 24, Germany (2021), p. 5, Israel (2021), p. 403, New Zealand (2020), para 10, Norway (2021), p. 4, Singapore (2021), p. 83, the UK (2018, 2021, para 9, and 2022) and the US (2016, pp. 13-14, 2020, and 2021, p. 140).

28 Common position of the AU (2024), para 31.

29 Common position of the AU (2024), para 32.

30 National position of Costa Rica (2023), para 24.

31 See Antonio Coco, Talita Dias, and Tsvetelina van Benthem, 'Illegal: The SolarWinds Hack under International Law' (2022) 33(4) *European Journal of International Law* 1275, 1280-1281.



While the prohibition of intervention only applies between States, a State might violate the obligation by supporting the coercive acts of non-State actors.³² Violations of the prohibition give rise to State responsibility.



c. Use of force

The prohibition of the use of force is enshrined in Article 2(4) of the UN Charter, which requires States to ‘refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations’.³³ This rule reflects customary international law,³⁴ and it has also been considered a peremptory norm of general international law (or *jus cogens*).³⁵ There is no doubt that it applies in the cyber context,³⁶ and as such it is a feature of virtually all published national and common positions.

As indicated by the phrase ‘in their international relations’, the prohibition of the use of force is **typically understood to apply only between States**.³⁷ This means that non-State actors – such as hacker groups, ransomware gangs, or rebel movements – are excluded from its scope unless their conduct is attributable to a State.³⁸ However, cyber operations by non-State actors that are not attributable to States but would otherwise amount to uses of force are not

There is no doubt that the prohibition of the use of force applies in the cyber context, and as such it features in virtually all national and common positions.

32 Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* (Chatham House 2019), para 79.

33 Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS 16 (UN Charter) Article 2(4).

34 ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) [2004] ICJ Rep 136 (Wall Advisory Opinion), para 87; ICJ, *Nicaragua Case*, paras 187–190. See also the national positions of *Brazil* (2021), p. 19, *Israel* (2021), pp. 398, *Sweden* (2022), p. 8 and the *US* (2021), p. 137.

35 See, for example, Christian Tams, ‘Article 2(4)’ in Bruno Simma et al (eds), *The Charter of the United Nations: A Commentary*, Vol I (OUP 2024) 359–360, para 137. See also the national positions of *Austria* (2024), p. 6, *Brazil* (2021), p. 19, *Cuba* (2024), para 12, *Czechia* (2024), para 24, and the common position of the *AU* (2024), para 38.

36 See, for example, UN 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), para 71(d).

37 See further Christian Tams, ‘Article 2(4)’ in Bruno Simma et al (eds), *The Charter of the United Nations: A Commentary*, Vol I (OUP 2024) 333–338, which argues that the scope of the prohibition also extends to ‘stabilized de facto regimes’ and to international organizations.

38 Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014), 44.

unregulated by international law. Such activities may give rise to individual criminal responsibility of the individuals concerned (see the section on international criminal law below) or implicate the due diligence obligations of States that fail to prevent, to halt, or to redress such operations (see the section on due diligence below).

The term **‘force’ is not defined in international law**, but there is a consensus that the characterization of a certain operation as a use of force does not depend on the means used. As the ICJ observed in its *Nuclear Weapons* advisory opinion, the prohibition applies ‘to any use of force, regardless of the weapons employed’.³⁹ This means that, in principle, the use of cyber capabilities may qualify as a use of force just as much as the resort to kinetic means may do. The prohibition also extends to threats to use force, which in the cyber context could include operations with the potential to result in the use of force or verbal threats conveyed online.⁴⁰

Rather than focusing on the means, the predominant approach for determining whether a cyber operation constitutes a use of force is by reference to its effects or consequences (the effects-based approach). On this basis, three broad categories of cyber operations have emerged:

- Many States hold that a cyber operation qualifies as a use of force if it produces **comparable effects to those of a conventional (kinetic) act** covered by the prohibition. This is straightforward if the cyber operation results in physical destruction or loss of life. Examples given in the published positions include severely damaging a power station,⁴¹ causing a train collision,⁴² or opening a dam above a populated area.⁴³
- It is less settled whether cyber operations that result in the **loss of functionality** of cyber infrastructure without causing material damage qualify as uses of force. As noted in Italy’s national position, such an interpretation could be justified because modern societies’ reliance on cyber technologies has made it possible to interrupt essential services without causing physical damage.⁴⁴ Examples given by States include significantly impairing critical infrastructure,⁴⁵ disabling or disrupting

39 ICJ, *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226 (Nuclear Weapons Advisory Opinion), para 39.

40 See Duncan B Hollis and Tsvetelina van Benthem, ‘Threatening Force in Cyberspace’, in Laura A Dickinson, and Edward W Berg (eds), *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold* (OUP 2024).

41 See the national positions of [Austria \(2024\)](#), p. 7, and [Poland \(2022\)](#), p. 5.

42 See the national position of [Israel \(2021\)](#), p. 399.

43 See the national position of the [US \(2012\)](#).

44 See the national position of [Italy \(2021\)](#), p. 8.

45 See the national position of [Ireland \(2023\)](#), para 18.



the functioning of electrical infrastructure,⁴⁶ or deactivating missile-defence systems.⁴⁷

- The qualification of cyber operations causing **purely economic harm** is even more controversial. Traditionally, the prohibition of the use of force was viewed as limited to armed force, excluding other forms of coercion (such as economic pressure), which would at most qualify as violations of the principle of non-intervention.⁴⁸ However, due to the potential of cyber operations to cause widespread and significant economic damage, several States have now expressed in their national positions their unwillingness to rule out that such cyber operations may qualify as a use of force. This is one of the issues on which the views of more States are needed.⁴⁹

The unsettled nature of these questions is evident in the recurrent affirmation by States that the assessment of whether a cyber operation qualifies as a use of force must be made on a case-by-case basis.⁵⁰ In this way, States maintain a degree of flexibility in this fast-evolving area. To promote legal certainty, States may consider identifying criteria for such determinations. The *Tallinn Manual 2.0* offers useful guidance in this regard, listing factors such as the severity, invasiveness, and military nature of the operation in question.⁵¹ Some States have already done that in their national positions.⁵²

A use of force is considered unlawful unless it is consented to by the territorial State,⁵³ authorized by the UN Security Council,⁵⁴ or conducted in self-defence.⁵⁵ **If a cyber use of force qualifies as an armed attack,⁵⁶ the victim State may invoke its right to self-defence,** and third States may

46 See the national positions of [Costa Rica \(2023\)](#), para 10, and [Norway \(2021\)](#), p. 6.

47 See the national position of [Poland \(2022\)](#), p. 5, and also the common position of the [AU \(2024\)](#), para 40.

48 Christian Tams, 'Article 2(4)' in Bruno Simma et al (eds), *The Charter of the United Nations: A Commentary*, Vol I (OUP 2024) 315, para 47. See also the national position of [Cuba \(2024\)](#), para 12.

49 See, for example, the national positions of [Denmark \(2023\)](#), p. 451, [France \(2019\)](#), p. 7, [the Netherlands \(2019\)](#), p. 4, and [Norway \(2021\)](#), p. 6.

50 See, for example, the national positions of [Canada \(2022\)](#), para 45, [Costa Rica \(2023\)](#), para 36, [Czechia \(2024\)](#), para 27, [Denmark \(2023\)](#), pp. 451–452, [Germany \(2021\)](#), p. 6, [Italy \(2021\)](#), p. 8, [the Netherlands \(2019\)](#), p. 4, [Norway \(2021\)](#), p. 5, [Poland \(2022\)](#), p. 5, [Romania \(2021\)](#), p. 77, [Sweden \(2022\)](#), p. 4, and the [US \(2021\)](#), p. 137, and also the common position of the [AU \(2024\)](#), para 41.

51 *Tallinn Manual 2.0*, commentary to Rule 69, para 9.

52 See, for example, the national positions of [Czechia \(2024\)](#), para 27, [Denmark \(2023\)](#), p. 451, [France \(2021\)](#), p. 7, [Germany \(2021\)](#), p. 6, [Norway \(2021\)](#), p. 5, [the Netherlands \(2019\)](#), p. 4, [Romania \(2021\)](#), p. 77, [Singapore \(2021\)](#), p. 84, and the [US \(2012 and 2021\)](#), p. 137), and also the common position of the [AU \(2024\)](#), para 41.

53 See, for example, the national positions of [Australia \(2021\)](#), p. 3, and [Romania \(2021\)](#), p. 77.

54 See [UN Charter](#), Articles 39–42.

55 See [UN Charter](#), Article 51.

56 See ICJ, *Nicaragua Case*, paras 191 and 195, which holds that only the 'most grave forms of the use of force' qualify as armed attacks and identifying 'scale and effects' as the criteria upon which to evaluate whether a use of force so qualifies.



use force in collective self-defence at its request.⁵⁷ The ICJ has clarified that only the ‘most grave forms of the use of force’ qualify as armed attacks and identified ‘scale and effects’ as the criteria on which to evaluate whether an act qualifies as a use of force. This approach is reflected in many national and common positions,⁵⁸ with that of the US as a notable outlier in asserting that all uses of force qualify as armed attacks.⁵⁹

As with kinetic uses of force, there is **no universally accepted threshold for determining which cyber uses of force qualify as armed attacks**. States generally agree that operations resulting in significant loss of life or substantial physical damage meet the threshold.⁶⁰ Examples given in published national positions include causing a nuclear reactor to malfunction, thereby causing serious damage and loss of life,⁶¹ or causing severe and prolonged outage of critical national infrastructure.⁶² In the cyber context as in other ones, there is ongoing debate over whether the conduct of non-State actors can constitute an armed attack, and thus trigger the victim State’s right to use force in self-defence in the territory of the State where the attack originated.⁶³

Any resort to self-defence must comply with the twin **requirements of necessity and proportionality**.⁶⁴ First, the use of force in self-defence must be necessary to repel the armed attack. Thus, if for example non-forcible passive cyber defences were sufficient for this purpose, the State would be precluded from using force.⁶⁵ Second, proportionality requires that the response does not exceed what is necessary to counter the attack. Importantly, the victim State is not obliged to respond in kind; it may use cyber or kinetic means, provided the requirements of necessity

57 See UN Charter, Article 51 and ICJ, *Nicaragua Case*, paras 195 and 199.

58 See, for example, the national positions of Austria (2024), p. 7, Brazil (2021), p. 20, Costa Rica (2023), para 37, Denmark (2023), pp. 451-452, Cuba (2024) para 6, Czechia (2024), para 29, France (2021), p. 5, Germany (2021), p. 15, Italy (2021), p. 9, the Netherlands (2019), p. 8, Norway (2021), p. 5, Sweden (2022), p. 4, Switzerland (2021), p. 4, and also the common positions of the AU (2024), para 41 and the EU (2024), p. 10.

59 See the national position of the US (2012).

60 See, for example, the national positions of Austria (2024), p. 7, France (2021), p. 5, Italy (2021), p. 8, New Zealand (2020), para 7, and the UK (2018).

61 See the national positions of New Zealand (2020), para 8, and the UK (2018).

62 See the national positions of France (2021), pp. 5-6, Norway (2021), p. 6, and Singapore (2021), p. 84.

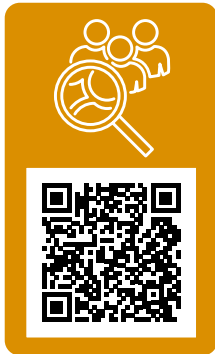
63 See, for example, the national positions of Austria (2024), p. 7-8, Denmark (2023), p. 452, Germany (2021), p. 16, Israel (2021), p. 399, Italy (2021), p. 9, the Netherlands (2019), p. 9, Poland (2022), p. 6, and the US (2021), p. 137, which all state that armed attacks may be perpetrated by non-State actors, whereas the national positions of Brazil (2021), p. 20 and France (2021), p. 6, argue that only States may commit armed attacks.

64 See ICJ, *Nicaragua Case*, para 176; ICJ, *Nuclear Weapons Advisory Opinion*, para 41; ICJ, *Case Concerning Oil Platforms (Iran v US)* (Judgment) [2003] ICJ Rep 161, para 74.

65 See, for example, the national position of the US (2021), p. 142.



and proportionality are met.⁶⁶ This flexibility ensures that the right to self-defence remains effective even when the perpetrator State does not depend on cyber capabilities.⁶⁷



d. Due diligence

‘Due diligence’ refers to a standard of conduct found in different international obligations, such as the positive human rights obligations discussed below. It is also shorthand for two obligations of general applicability in international law.

The first is the principle formulated by the ICJ in the *Corfu Channel* case, which recognizes ‘every State’s **obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States**’.⁶⁸

This general obligation of prevention is grounded in customary international law and is a corollary of State sovereignty.⁶⁹ It may be breached when a State knows or should have known that an act contrary to the rights of another State originates in or is perpetrated through its territory, and yet fails to take reasonable action to stop or prevent it, and the harm materializes.⁷⁰

The second general obligation of due diligence is the ‘**no-harm**’ principle found in customary international law⁷¹ and reflected in the International Law Commission (ILC) Draft Articles on Prevention of Transboundary Harm from Hazardous Activities.⁷² This is an obligation to ‘take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof’, where such harm originates in a State’s territory or jurisdiction and significantly affects persons, property, or the environment

66 See, for example, the national positions of Austria (2024), p. 7, Canada (2022), para 47, Estonia (2021), p. 30, Finland (2020), p. 7, France (2021), p. 6-7, Germany (2021), p. 15, Israel (2021), p. 399, the Netherlands (2019), p. 8, New Zealand (2020), para 24, Norway (2021), p. 9, Poland (2022), p. 5, Sweden (2022), p. 4, the UK (2021), para 6, and the US (2021), p. 137.

67 See the national position of Poland (2022), p. 5.

68 ICJ, *Corfu Channel Case (UK v Albania)* (Merits) [1949] ICJ Rep 4, 22.

69 See ICJ, *Pulp Mills on the River Uruguay (Argentina v Uruguay)* (Judgment) [2010] ICJ Rep 14, para 101; *Island of Palmas (US v Netherlands)* (1928) II RIAA 829, 839.

70 See Council of the European Union, *Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace* (2024), 5; Talita Dias and Antonio Coco, *Cyber Due Diligence in International Law* (ELAC 2021) 784–789. For the *Tallinn Manual 2.0* experts, the following cumulative criteria must be fulfilled: the existence of an act contrary to the rights of a victim State, that act must be conducted from or through the infrastructure under the control of the responsible State, that act would have been unlawful if conducted by the State itself, that act has serious adverse consequences; the State has actual or constructive knowledge, and the State fails to take feasible measures to stop that act. See *Tallinn Manual 2.0*, commentary to Rule 6.

71 See *Trail Smelter Case (US v Canada)* (1941) 3 RIAA 1911, at 1963; ICJ, *Pulp Mills on the River Uruguay (Argentina v Uruguay)* (Judgment) [2010] ICJ Rep 14, paras 101, 187, 197, 204, 223.

72 ILC, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries*, A/56/10 (2001).



in another State.⁷³ While the scope of the ILC Draft Articles was limited to activities causing physical harm,⁷⁴ the no-harm principle was never meant to be restricted to ecological matters.⁷⁵ On one view, the no-harm principle also applies to non-physical harm, such as financial or reputational harm against a State.⁷⁶

In the cyber context, the GGE has recognized that ‘States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs’.⁷⁷ However, **whether due diligence constitutes a binding obligation applicable to cyber operations remains controversial.**

For some States, due diligence is simply a non-binding norm in the cyber context.⁷⁸ They have pointed to how due diligence has been framed as a non-binding voluntary norm of responsible State behaviour by the GGE and the insufficient State practice supporting the existence of such an obligation in the cyber context. The reluctance to accept that due diligence is applicable in the cyber context seems to stem from a concern that States might not be able to prevent or stop malicious cyber operations given their often covert and rapid nature. For example, it would be difficult to prevent the exploitation of harmful hidden functions in software in the absence of knowledge thereof. There is also a concern that accepting due diligence as a binding obligation would lead to frequent breaches of the obligation, inviting countermeasures and increasing the risk of conflict escalation in cyberspace.

However, a significant number of States have accepted in their national positions that the *Corfu Channel* principle is applicable and therefore binding in the cyber as in other contexts.⁷⁹ A few other States have also endorsed the applicability of the no-harm principle in the cyber context.⁸⁰

73 ILC, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries*, A/56/10 (2001), Articles 2 and 3.

74 ILC, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries*, A/56/10 (2001), commentary to Article 1, paras-16-17.

75 UN, *Fourth report on international liability for injurious consequences arising out of acts not prohibited by international law*, by Robert O. Quentin-Baxter, *Special Rapporteur*, A/ CN.4/373 and Corr.1&2 (27 June 1983), para 17.

76 See, for example, the national position of Czechia (2024), para 18; Talita Dias and Antonio Coco, *Cyber Due Diligence in International Law* (ELAC 2021) 790–794.

77 UN General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/70/174 (22 July 2015), para 13(c).

78 See, for example, the national positions of Canada (2022), paras 26-27, Israel (2021), p. 404, New Zealand (2020), para 16, and the UK (2021), para 12.

79 See, for example, the national positions of Austria (2024), p. 10, Colombia (2025), p. 9, Estonia (2019 and 2021, p. 26), Finland (2020), p. 4, France (2019), p. 10, Germany (2021), p. 3, Italy (2021), p. 6, Japan (2021), p. 5, the Netherlands (2019), p. 4, Switzerland (2021), p. 7, and Sweden (2022), p. 4, and also the common positions of the AU (2024), para 21 and the EU (2024), p. 5

80 See the national positions of Costa Rica (2023), para 29, Czechia (2024), para 18, and Norway (2021), p. 7.



This view is motivated by the need to close the accountability gap that could result from the difficulty of attributing cyber operations to States and the ever-increasing use of proxies in the cyber context. After all, due diligence would hold States responsible for failing to prevent, stop, or redress harmful cyber operations carried out by non-State actors or third States from their territory or ICT infrastructure. This includes activities carried out by cyber criminals, such as ransomware and IT supply chain attacks.

States that have endorsed due diligence as a binding obligation have stressed that **the obligation is one of conduct rather than result**: States must take reasonable measures to prevent, stop, or redress malicious cyber operations carried out from or through their territory or infrastructure. In their national positions, these States have also highlighted that the obligation is subject to a requirement of actual or constructive knowledge as well as the capacity to take feasible action in the circumstances.⁸¹ Therefore, due diligence would not pose an insurmountable burden on States, especially developing countries, by requiring, for example, the constant monitoring of cyber activities or the prevention of all malicious cyber activities taking place in a State's territory.

There is agreement that the topic of due diligence requires further study. This is particularly the case for what due diligence means in practice; that is, the various measures that States may be required to adopt to prevent, stop, or redress malicious cyber activity. Examples of such measures can be found in several norms of responsible State behaviour laid out by the GGE, such as norms 'g' (on the protection of critical infrastructure), 'h' (on responses to requests for assistance by other States), and 'j' (on responsible reporting of ICT vulnerabilities).⁸² Other examples of diligent behaviour include enacting and enforcing a legal framework for cybercrime and other cyber threats, the establishment of a computer emergency response team (CERT), carrying out cyber risk assessments, and developing public-private partnerships to enhance cybersecurity.⁸³

There is agreement that due diligence requires further study, particularly regarding what practical measures States must take to prevent, stop, or redress malicious cyber activity.

81 See, for example, the national positions of Austria (2024), p. 10, Czechia (2020 and 2024, para 15), Estonia (2019 and 2021, p. 26), Ireland (2023), para 13, and Japan (2021), p. 5, and also the common positions of the AU (2024), para 23 and the EU (2024), p. 5

82 See UN General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/70/174 (22 July 2015), para 13.

83 See Talita Dias and Antonio Coco, *Cyber Due Diligence in International Law* (ELAC 2021) 165–205.



e. Peaceful settlement of disputes

The peaceful settlement of disputes is a foundational principle of international law, enshrined in the UN Charter⁸⁴ and reflective of customary international law.⁸⁵ It is a corollary of the prohibition of the use of force and is a binding obligation on States to resolve their international disputes by peaceful means.⁸⁶ This obligation is widely recognized to apply in the cyber context,⁸⁷ consistent with the frequently reaffirmed commitment of States to promote an ‘open, secure, stable, accessible and *peaceful* ICT environment’.⁸⁸

However, there are variations in how this obligation is articulated in national positions. Some interpret it broadly to cover any international dispute,⁸⁹ a view supported by the plain wording of Article 2(3) of the UN Charter, which imposes no additional conditions.⁹⁰ Others limit the obligation to disputes ‘likely to endanger international peace and security’.⁹¹ This criterion, found in Article 33(1) of the UN Charter, is also relied upon by the Tallinn Manual 2.0 to limit the scope of the obligation as a whole.⁹²

The choice of means for dispute settlement remains with the parties,⁹³ with the UN Charter providing examples such as negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, and resort to regional agencies

84 UN Charter, Articles 2(3) and 33.

85 ICJ, *Nicaragua Case*, para 290.

86 Alain Pellet, ‘Peaceful Settlement of International Disputes’ in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (online edn, OUP 2013), paras 2–3.

87 UN General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/70/174 (22 July 2015), para 28(b) and UN 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), para 71(a). See also the national positions of *Austria* (2024), p. 11, *Canada* (2022), para 41, *China* (2021), p. 3, *Colombia* (2025), p. 10, *Costa Rica* (2023), para 17, *Czechia* (2024), para 21, *Estonia* (2021), p. 29, *France* (2019), p. 2, *Japan* (2021), p. 6, *Kenya* (2021), p. 54, *Singapore* (2021), p. 85, *Switzerland* (2021), p. 2, and the *UK* (2021, para 7, and 2022).

88 See, for example, the national positions of *Brazil* (2021), p. 17, *Colombia* (2025), p. 4, *Estonia* (2021), p. 23, *Finland* (2020), p. 1, *Ireland* (2023), para 2, *Italy* (2021), p. 3, *Kenya* (2021), p. 52, *New Zealand* (2020), para 1, *Norway* (2020), p. 1, *Pakistan* (2023), para 7, *Singapore* (2021), p. 83, *Sweden* (2022), p. 1, *Switzerland* (2021), p. 1, and the *UK* (2021), para 1, and also the common position of the *AU* (2024), para 3. (Emphasis added.)

89 See, for example, the national positions of *Canada* (2022), para 41, *Costa Rica* (2023), para 17, *Czechia* (2024), para 21, *Japan* (2021), p. 6, and *Singapore* (2021), p. 85, and also the common positions of the *AU* (2024), para 35, and the *EU* (2024), p. 9.

90 Christian Tomuschat, ‘Article 2(3)’ in Bruno Simma et al (eds), *The Charter of the United Nations: A Commentary*, Vol I (OUP 2024), 283, para 42.

91 See, for example, the national positions of *Austria* (2024), p. 11, *Estonia* (2021), p. 29, and *Switzerland* (2021), p. 2.

92 *Tallinn Manual 2.0*, commentary to Rule 65, para 2.

93 ICJ, *Fisheries Jurisdiction (Spain v Canada)* (Jurisdiction of the Court) [1998] ICJ Rep 432, para 56.



or arrangements.⁹⁴ This list is non-exhaustive, and States may also employ other appropriate peaceful means or combine several ones.⁹⁵ However, as affirmed by the 1982 Manila Declaration, they must do so in good faith and in a spirit of co-operation.⁹⁶ In accordance with the UN Charter, the UN Security Council may also call upon the parties to settle the dispute by peaceful means if it is likely to endanger the maintenance of international peace and security.⁹⁷

In the cyber context, disputes between States may encompass factual and legal dimensions:

- **Factual disputes** in cyberspace often focus on technical attribution; that is, identifying which machine was used to carry out a particular cyber operation and determining the individual(s) or groups involved. They may also involve questions about the effects of the operation, the timing of its execution, or whether one took place at all. In this respect, fact-finding mechanisms are important.⁹⁸ It is conceivable that formal attribution mechanisms will be developed in the future to address these challenges.⁹⁹
- **Legal disputes** typically relate to whether a cyber activity that adversely affects one State is legally attributable to another, and whether it constitutes a breach of any applicable rule of international law. Such disputes may be submitted to judicial settlement, including to the ICJ as the principal judicial organ of the UN. Provided jurisdiction and admissibility requirements are met, the ICJ is competent to adjudicate disputes on any issue of international law, which includes the application of international law to cyber activities.

⁹⁴ UN Charter, Article 33(1).

⁹⁵ Alain Pellet, 'Peaceful Settlement of International Disputes' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (online edn, OUP 2013), para 31.

⁹⁶ UN General Assembly, *Manila Declaration on the Peaceful Settlement of International Disputes*, A/RES/37/10 (15 November 1982), section I, para 5.

⁹⁷ UN Charter, Article 33(2).

⁹⁸ Nicholas Tsagourias, 'Cyber Disputes as International Legal Disputes', in Nicholas Tsagourias, Russell Buchan, and Daniel Franchini (eds), *Peaceful Settlement of Inter-State Cyber Disputes* (Hart 2024), 20.

⁹⁹ See, for example, Yuval Shany and Michael N Schmitt, 'An International Attribution Mechanism for Hostile Cyber Operations' (2020) 96 *International Law Studies* 196.



States may wish to use their national positions to articulate views on how factual and legal international disputes involving ICTs should be resolved. This could include expressing views on the possible creation of attribution or other fact-finding mechanisms,¹⁰⁰ encouraging other States to accept the ICJ's compulsory jurisdiction or refraining from doing so,¹⁰¹ and exploring how ICTs can be used to help settle cyber and non-cyber disputes peacefully.¹⁰²

During multilateral discussions on State uses of ICTs and international security, some States have raised concerns that the characteristics of cyberspace may encourage unilateral measures over peaceful dispute resolution.¹⁰³ On the one hand, it is true that the obligation to seek the peaceful settlement of disputes does not impair other rights of States under international law, including the right to take lawful countermeasures and the right to use force in self-defence in response to an armed attack.¹⁰⁴ On the other hand, as explained above, any resort to those unilateral measures is only available under strict conditions. If those criteria are not met, States must engage in good-faith efforts to resolve disputes through peaceful means. In any case, they must refrain from any measures that would endanger international peace and security.¹⁰⁵

In the cyber context, inter-State disputes may concern both facts (e.g. technical attribution) and law (e.g. legal attribution or qualification of operations as breaches of international law).

100 See, for example, the national position of [Cuba \(2024\)](#), paras 23-24.

101 See, for example, the national positions of [Switzerland \(2021\)](#), p. 2, and the [UK \(2022\)](#).

102 See, for example, common position of the [AU \(2024\)](#), para 37.

103 UN General Assembly, *Chair's Summary of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, [A/AC.290/2021/CRP.3](#) (10 March 2021), para 7.

104 See, for example, the national positions of [Canada \(2022\)](#), para 42, [Czechia \(2024\)](#), para 23, [Estonia \(2021\)](#), p. 29, [Singapore \(2021\)](#), p. 85.

105 [UN Charter](#), Article 2(3). See also [Tallinn Manual 2.0](#), commentary to Rule 65, para 12.



f. Self-determination

The right to self-determination has been recognized by the UN General Assembly as one of the ‘basic principles of international law’.¹⁰⁶ It is enshrined in the UN Charter,¹⁰⁷ the International Covenant on Civil and Political Rights (ICCPR),¹⁰⁸ and the International Covenant on Economic, Social and Cultural Rights (ICESCR).¹⁰⁹ Moreover, it is widely regarded as reflecting customary international law.¹¹⁰ The corresponding obligation to respect this right is considered to be an obligation owed to the international community as a whole,¹¹¹ and it is potentially a peremptory norm of general international law (*jus cogens*).¹¹²

While the right to self-determination is a fundamental human right,¹¹³ it differs from the other rights discussed in the international human rights law section below in that it is a **collective right**. The right-holder is not an individual but a defined group, commonly referred to as ‘a people’. Although international law does not formally define ‘a people’, the term is generally understood to refer to a group with a shared historical, cultural, or linguistic heritage and a connection to a specific territory, which also self-identifies as such.¹¹⁴

Self-determination can be divided into internal and external dimensions. **Internal self-determination** refers to a people’s right to freely pursue its political, economic, social, and cultural development within the framework of an existing State.¹¹⁵ **External self-determination** involves the right of a people to determine its international status, such as achieving

106 UN 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) (24 October 1970) Annex.

107 UN Charter, Article 1(2).

108 ICCPR, Article 1.

109 ICESCR, Article 1.

110 ICJ, *Legal Consequences of the Separation of the Chagos Archipelago from Mauritius in 1965* (Advisory Opinion) [2019] ICJ Rep 95 (*Chagos Advisory Opinion*), para 155.

111 ICJ, *East Timor (Portugal v Australia)* (Judgment) [1995] ICJ Rep 90, para 29; ICJ, *Wall Advisory Opinion*, para 88.

112 See, for example, ILC, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries* (2001) (ARSIWA), commentary to Article 26, para 5; ICJ, *Chagos Advisory Opinion*, Separate Opinion of Judge Robinson, para 77; ICJ, *Legal Consequences Arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, Including East Jerusalem* (Advisory Opinion) (19 July 2024), para 233 (limiting this finding to situations of foreign occupation).

113 ICJ, *Chagos Advisory Opinion*, para 144.

114 Milena Sterio, *The Right to Self-Determination under International Law* (Routledge 2013), 16; Tom Sparks, *Self-Determination in the International Legal System* (Bloomsbury 2023), 24.

115 UN General Assembly, *Declaration on the Granting of Independence to Colonial Countries and Peoples*, Res 1514 (XV) (14 December 1960) 2; ICJ, *Legal Consequences Arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, Including East Jerusalem* (Advisory Opinion) (19 July 2024), para 241.



independence as a sovereign State or choosing to integrate with another State.¹¹⁶ It is generally accepted that the right to external self-determination arises only in exceptional circumstances, such as when a people is subject to oppression or colonial domination.¹¹⁷

At the time of writing, only three national positions address the right to self-determination. Italy's refers to the right to internal self-determination as an 'ancillary rule' to the principle of sovereignty.¹¹⁸ Similarly, Iran's states that sovereignty must be 'interpreted under the other fundamental legal principles', including self-determination.¹¹⁹ Russia's also recognizes the applicability of 'self-determination of peoples' in the cyber context, though without elaboration.¹²⁰

States may wish to clarify several aspects of the right to self-determination in the cyber context in their national or common positions.

First, it has been argued that **cyber interference with electoral processes in another State** may be inconsistent with the internal dimension of the right to self-determination.¹²¹ While such interference may simultaneously qualify as a violation of the principles of sovereignty and/or non-intervention, States may wish to clarify the dividing lines between these concepts and how to reconcile them in case of norm conflict. For instance, foreign interference in support of democratic self-government in a State with an authoritarian regime may be in tension with the principle of sovereignty but consistent with the principle of self-determination.¹²²

At the time of writing, few national positions address the right to self-determination. However, several of its dimensions may be implicated by cyber operations and could be usefully addressed in future positions.

116 Karen Knop, *Diversity and Self-Determination in International Law* (CUP 2009), 18.

117 See, for example, *Reference re Secession of Quebec* [1998] 2 SCR 217, para 112.

118 National position of [Italy](#) (2021), p. 4.

119 National position of [Iran](#) (2020), para II.5.

120 National position of [Russia](#) (2021), p. 79.

121 See, for example, Nicholas Tsagourias, 'Electoral Cyber Interference, Self-Determination and the Principle of Non-intervention in Cyberspace', in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy* (Rowman & Littlefield 2020); Marco Roscini, *International Law and the Principle of Non-Intervention* (OUP 2024) 399–400.

122 Jens D Ohlin, 'Did Russian Cyber-Interference in the 2016 Election Violate International Law?' (2017) 95 *Texas Law Review* 1579, 1597.



Second, it is generally accepted that the right to self-determination includes **the right to exercise permanent sovereignty over natural resources**.¹²³

As noted by UN Secretary General António Guterres, '[d]igital technologies today are similar to natural resources such as air and water'.¹²⁴ At the same time, States have recognized in the Global Digital Compact that some technologies, including open-source software and open data, are to be considered 'digital public goods' or digital public infrastructure.¹²⁵ States may therefore need to consider which digital technologies or elements of the digital space, such as access to global communication networks or the equitable allocation of IP addresses, constitute resources subject to permanent sovereignty or digital public goods. A consequence of considering that such technologies are subject to sovereignty is that the denial of such access could, in certain circumstances, constitute a violation of self-determination.

Third, the right to self-determination **protects peoples against acts designed to disperse the population and undermine its integrity as a people**.¹²⁶ In the cyber context, this might include large-scale disinformation campaigns designed to compel population movement and alter the demographic composition of a territory. Another possible example is the imposition of internet shutdowns on a people by the controlling State, depriving communities of access to vital services and disrupting social cohesion. States may wish to articulate the extent to which such cyber acts fall within the scope of the right to self-determination.

123 ICJ, *Case Concerning Armed Activities in the Territory of the Congo (Democratic Republic of Congo v Uganda)* (Merits) [2005] ICJ Rep 168, para 244; ICJ, *Legal Consequences Arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, Including East Jerusalem* (Advisory Opinion) (19 July 2024), para 240.

124 UN General Assembly, *Our Common Agenda Policy Brief 5: A Global Digital Compact – An Open, Free and Secure Digital Future for All*, A/77/CRP.1/Add.4 (25 April 2023), para 31.

125 UN General Assembly, *Global Digital Compact*, A/79/L.2 (2024), para 14.

126 ICJ, *Legal Consequences Arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, Including East Jerusalem* (Advisory Opinion) (19 July 2024), para 239.

3. Specialized regimes

This section explores how three specialized regimes of international law – international humanitarian law (IHL), international human rights law (IHRL), and international criminal law (ICL) – apply to cyber activities. These have been selected because they are frequently addressed in the national positions issued to date, although other specialized regimes too have occasionally been included in positions.¹²⁷ Each regime provides a distinct legal framework governing cyber activities that fall within its scope. What unites them is their shared focus on the protection of individuals from harm, including harm resulting from the use of modern technologies such as cyber capabilities.



a. International humanitarian law

IHL is a body of rules that seeks to limit the effects of armed conflict for humanitarian reasons. It establishes limits on the conduct of parties to conflict and on States more broadly, thereby protecting victims of armed conflicts, including civilians and the civilian population. In the 2010s, there was some debate among States over **whether IHL applied to cyber operations**.¹²⁸ However, following the adoption of the GGE report in 2021 and its subsequent endorsement by the UN

General Assembly and the OEWG, there is now a broad consensus that this is the case and that affirming this applicability does not legitimize conflict or encourage militarization.¹²⁹ All national positions that address IHL, including those issued by previously sceptical States,¹³⁰ have endorsed this view as

127 See, for example, the national position of Austria (2024), p. 14, which includes a section on diplomatic and consular law.

128 Anders Henriksen, 'The end of the road for the UN GGE process: The future regulation of cyberspace' (2019) 5(1) *Journal of Cybersecurity* 1; Eneken Tikk and Mika Kerttunen, *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*, Cyber Policy Institute (2017).

129 See UN 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) para 71(f); UN General Assembly, *Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025*, A/79/214 (22 July 2024), para 36(b)(ii). See also 34th International Conference of the Red Cross and Red Crescent, *Resolution 2: Protecting Civilians and Other Protected Persons and Objects Against the Potential Human Cost of ICT Activities During Armed Conflict*, 34IC/24/R2 (October 2024).

130 See, for example, Cuba's Representative Office Abroad, '71 UNGA: Cuba at the final session of the Group of Governmental Experts on the developments in the field of information and telecommunications in the context of international security' (23 June 2017).



a starting point.¹³¹ Accordingly, the focus of international discussions has shifted to how IHL applies in the cyber context.

There is now a broad consensus among States that IHL applies to cyber operations during armed conflicts and that affirming this applicability does not legitimize conflict or encourage militarization.

While the majority of IHL rules apply during armed conflict, **certain obligations must also be observed or implemented in peacetime**. These include the duty to respect and ensure respect for IHL;¹³² the obligation to disseminate IHL as widely as possible, including through instruction to armed forces;¹³³ the obligation to carry out legal reviews of new weapons, means, and methods of warfare;¹³⁴ and the duty to prevent and repress the misuse of protective emblems such as the red cross, red crescent, and red crystal.¹³⁵ While most published positions provide little or no detail on these peacetime obligations, highlighting their relevance in the cyber context offers an opportunity for States not anticipating involvement in armed conflict to emphasize the importance of IHL.

The **relationship between cyber operations and armed conflicts** can take one of two forms. On the one hand, cyber operations may be carried out as part of an existing armed conflict. Provided that these operations have a nexus to the conflict, they are governed and therefore limited by IHL. On the other hand, cyber operations may conceivably bring an armed conflict into existence where none previously existed. In such cases, the emergence of the armed conflict triggers the application of IHL to all conduct with a nexus to it. IHL distinguishes between international and non-international armed conflicts.

131 See the national positions of Australia (2021), p. 3, Austria (2024), p. 16, Brazil (2021), p. 22, Canada (2022), para 48, Costa Rica (2023), para 38, Cuba (2024) para 16, Czechia (2020 and 2024, para 37), Denmark (2023), p. 454, Estonia (2021), p. 26, Finland (2020), p. 7, France (2019), p. 13, Germany (2021), p. 7, Ireland (2023), para 29, Israel (2021), p. 399, Italy (2021), p. 9, Japan (2021), p. 6, Kenya (2021), p. 54, Netherlands (2019), p. 5, New Zealand (2019), para 25, Norway (2021), p. 9, Pakistan (2023), para 9, Poland (2022), p. 7, Romania (2021), p. 77, Singapore (2021), p. 85, Sweden (2022), p. 6, Switzerland (2021), p. 8, the UK (2018 and 2021, para 22), and the US (2012, 2016, p. 8, 2020, and 2021, p. 138), and also the common positions of the AU (2024), para 47, and the EU (2024), p. 2.

132 Common Article 1 to the 1949 Geneva Conventions; Additional Protocol I, Article 1(1); Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law: Volume I, Rules* (ICRC and CUP 2005) (ICRC Customary IHL Study) Rules 139 and 144; 26th International Conference of the Red Cross and Red Crescent, *Resolution 1: International Humanitarian Law – From Law to Action*, 26IC/95/R1 (3 December 1995), para 2.

133 Geneva Conventions I/II/III/IV, Articles 47/48/127/144; Additional Protocol I, Article 83; Additional Protocol II, Article 19.

134 Additional Protocol I, Article 36.

135 See Geneva Convention I, Articles 53–54.



- An **international armed conflict** arises when armed force is used between two or more States.¹³⁶ This criterion is generally understood not to require a specific level of intensity.¹³⁷ Therefore, there is broad agreement that cyber operations with effects comparable to kinetic operations may give rise to an international armed conflict.¹³⁸



- A **non-international armed conflict** is characterized by fighting between a State and an organized non-State armed group or between such groups. The identification of a non-international armed conflict can be more complex as it requires meeting a higher threshold of intensity.¹³⁹ Whether cyber operations, particularly those without kinetic effects, can meet this threshold remains unsettled.¹⁴⁰ Nonetheless, a few national positions as well as the common position of the AU affirm that cyber operations could trigger a non-international armed conflict.¹⁴¹ This remains an issue with respect to which the views of more States are needed.



Further key questions that require the attention of States relate to the scope of the **prohibition of attacks against civilians and civilian objects**. This prohibition, codified in Additional Protocol I to the Geneva Conventions and reflective of customary international law,¹⁴² applies – like the rest of IHL – to cyber operations during armed conflict. However, the interpretation of the terms ‘attacks’ and ‘objects’ in the cyber context remains debated.

136 ICJY, *Prosecutor v Tadić* (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) ICJY-94-1-A (2 October 1995) para 70.

137 ICRC, *How is the term “armed conflict” defined in international humanitarian law?*, Opinion Paper (2024) 9.

138 ICRC (ed), *Commentary on the Third Geneva Convention* (CUP 2021), commentary on Article 2, para 288.

139 See, for example, ICJY, *Prosecutor v Limaj* (Trial Judgment) ICJY-03-66-T (30 November 2005) para 84; ICJY, *Prosecutor v Boškoski and Tarčulovski* (Trial Judgment) ICJY-04-82-T (10 July 2008) para 175.

140 ICRC (ed), *Commentary on the Third Geneva Convention* (CUP 2021), commentary on common Article 3, para 471; Permanent Mission of Lichtenstein to the United Nations, *The Council of Advisers’ Report on the Application of the Rome Statute to Cyberwarfare* (August 2021), 33–36.

141 See, in particular, the national positions of Austria (2024), p. 17, Costa Rica (2023), para 43, France (2019), p. 12, Germany (2021), p. 7, and Ireland (2023), para 30, and also the common position of the AU (2024), para 49.

142 Additional Protocol I, Article 52(1); *ICRC Customary IHL Study*, Rules 1 and 7.



- First, a central issue is determining **when cyber operations qualify as 'attacks'** under IHL, which is a critical reference point for many rules governing the conduct of hostilities. In addition to the prohibition of attacks against civilians and civilian objects, these include the prohibition of indiscriminate attacks,¹⁴³ the prohibition of disproportionate attacks,¹⁴⁴ and the obligation to take all feasible precautions to avoid or at least reduce incidental harm to civilians and damage to civilian objects when carrying out an attack.¹⁴⁵ Article 49 of Additional Protocol I defines attacks as 'acts of violence against the adversary, whether in offence or in defence'. Assuming that an attack can be defined by its effects,¹⁴⁶ cyber operations causing violent effects such as death, injury, or damage would constitute attacks.¹⁴⁷ However, debate persists over whether cyber operations causing loss of functionality, without physical damage to the target systems, also qualify. A growing number of States endorse an interpretation that includes the loss of functionality,¹⁴⁸ while others limit the qualification of attacks to operations that are expected to cause physical harm.¹⁴⁹ Nevertheless, there seems to be agreement that a cyber operation may constitute an attack when loss of functionality is expected to cause physical damage, injury, or death.¹⁵⁰ This would be the case of a cyber operation that is intended to shut down electricity in a military airfield and, as a result, is expected to cause the crash of a military aircraft.¹⁵¹ Given the potentially severe impact of cyber operations on essential services, even without physical damage, clarifying the boundary between attacks and other cyber operations is crucial.
- Second, there is also ongoing debate about the protection of civilian data – such as social security, taxation, or electoral databases – as a civilian 'object'. Under IHL, all objects are protected from attack, including through cyber means, unless they qualify as



143 Additional Protocol I, Article 51(4); *ICRC Customary IHL Study*, Rules 11 and 12.

144 Additional Protocol I, Articles 51(5)(b) and 57; *ICRC Customary IHL Study*, Rule 14.

145 Additional Protocol I, Article 57; *ICRC Customary IHL Study*, Rule 15

146 Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94(886) *International Review of the Red Cross* 533, 557.

147 See *Tallinn Manual 2.0*, Rule 92.

148 See, for example, the national positions of [Austria \(2024\)](#), p. 17, [Colombia \(2025\)](#), p. 13, [Costa Rica \(2023\)](#), para 20, [France \(2019\)](#), p. 13, [Germany \(2021\)](#), p. 8, [Japan \(2021\)](#), p. 7, and [New Zealand \(2020\)](#), para 20.

149 See, for example, the national positions of [Denmark \(2023\)](#), p. 455, and [Israel \(2021\)](#), pp. 400-401.

150 *Tallinn Manual 2.0*, commentary to Rule 92, para 15.

151 National position of [Israel \(2021\)](#), pp. 400-401.



military objectives, as defined in Article 52(2) of Additional Protocol I.¹⁵² This raises the question of **whether civilian data qualifies as a civilian object** and thus benefits from IHL protections. Some States take the view that data, being allegedly immaterial, invisible, and intangible, cannot be considered an object under IHL.¹⁵³ However, this interpretation has been criticized for leaving cyber operations targeting civilian data outside the scope of those conduct of hostilities rules that pertain solely to civilian objects, thereby creating a significant protection gap.¹⁵⁴ An alternative perspective advocates a broader interpretation of the term 'object', aligning it with IHL's overarching humanitarian purpose.¹⁵⁵ This is because cyber operations interfering with civilian data can disrupt government services, harm private businesses, and affect individuals, underscoring the need to extend IHL protections to such data.¹⁵⁶ Accordingly, a growing number of States take the view that the protection of civilian objects extends to civilian data.¹⁵⁷

Even if certain **cyber operations fall outside of the scope of the prohibition of attacks against civilians and civilian objects**, they are not unregulated by IHL. Relevant rules include the obligation to exercise constant care to spare the civilian population and civilian objects during military operations.¹⁵⁸ Additional restrictions prohibit operations directed against specifically protected objects, such as medical facilities¹⁵⁹ and objects used for humanitarian relief operations,¹⁶⁰ and forbid operations designed to disable objects indispensable to the survival of the civilian population, such as water supply systems or agricultural infrastructure.¹⁶¹

152 See Additional Protocol I, Article 52(2): 'In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.'

153 See, for example, the national positions of [Denmark \(2023\)](#), p. 455, and [Israel \(2021\)](#), p. 401. See also [Tallinn Manual 2.0](#), commentary to Rule 100, para 5.

154 Kubo Mačák and Laurent Gisel, 'The Legal Constraints of Cyber Operations in Armed Conflicts', in Rajeswari Pillai Rajagopalan (ed), [Future Warfare and Technology: Issues and Strategies](#) (Wiley 2022) 148.

155 See, for example, Robert McLaughlin, 'Data as a Military Objective', Australian Institute of International Affairs (20 September 2018).

156 See further Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 [Israel Law Review](#) 55.

157 See, for example, the national positions of [Austria \(2024\)](#), p. 18, [Colombia \(2025\)](#), p. 18, [Costa Rica \(2023\)](#), para 50, [Finland \(2020\)](#), p. 7, [Germany \(2021\)](#), p. 8, and [Romania \(2021\)](#), p. 78.

158 The application of this rule to cyber operations has been affirmed by in the national position of States including [Austria \(2024\)](#), p. 18, [Czechia \(2024\)](#), para 42, [Costa Rica \(2023\)](#), para 52, [Denmark \(2023\)](#), p. 455, [Finland \(2020\)](#), p. 7, [France \(2019\)](#), p. 15, and [Germany \(2021\)](#), p. 9.

159 See Geneva Convention I, Article 19; Geneva Convention IV, Article 18; Additional Protocol I, Article 12; Additional Protocol II, Article 11(1); [ICRC Customary IHL Study](#), Rule 28.

160 Geneva Convention IV, Article 59(3); Additional Protocol I, Article 70(4); [ICRC Customary IHL Study](#), Rule 32.

161 Additional Protocol I, Article 54; Additional Protocol II, Article 14; [ICRC Customary IHL Study](#), Rule 54. See also UN Security Council, Res 2573 (2021) S/RES/2573 (27 April 2021).



Thus, IHL continues to impose significant constraints on how a cyber operation may be conducted even when it does not qualify as an attack or when the data it targets is not considered a civilian object. Clarifying these constraints offers an opportunity for States developing their national or common positions to further strengthen the protection of civilians from harm caused by cyber operations during armed conflict.



b. International human rights law

There is now consensus that human rights apply online just as they do offline.¹⁶² This means that States must respect, protect, and fulfil human rights in cyberspace, in accordance with their obligations under human rights treaties and customary international law.¹⁶³ Human rights treaties include the ICCPR and the ICESCR, alongside regional treaties such as the European Convention on Human Rights (ECHR), the American Convention on Human Rights (ACHR), and the African

Charter on Human and Peoples' Rights (ACHPR).¹⁶⁴ All these provide for judicial or quasi-judicial human rights monitoring bodies, namely the Human Rights Committee (for the ICCPR); the Committee on Economic, Social and Cultural Rights (for the ICESCR); the European Court of Human Rights (for the ECHR); the Inter-American Court of Human Rights (for the ACHR); and the African Court on Human and Peoples' Rights (for the ACHPR).

International treaties and customary international law¹⁶⁵ recognize a wide range of **human rights that are particularly relevant in the digital age**, including the freedoms of opinion, expression, and assembly as well as the rights to privacy and non-discrimination. Given the increasing digitalization of public services, the rights to life, health, and education as well as to just and favourable work conditions may also be affected by malicious conduct in

¹⁶² See, for example, UNHRC, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/32/13 (1 July 2016), para 1; UN General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/70/174 (22 July 2015), para 28(b).

¹⁶³ HRC, *General Comment No 31 [80]: The nature of the general legal obligation imposed on States Parties to the Covenant*, CCPR/C/21/Rev.1/Add.13 (26 May 2004) (General Comment 31), paras 6–8.

¹⁶⁴ International Covenant on Civil and Political Rights (16 December 1966) 999 UNTS 171; International Convention on the Elimination of All Forms of Racial Discrimination (21 December 1965) 660 UNTS 195; European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, ETS 5, (4 November 1950); American Convention on Human Rights, Treaty Series, No 36 (1969); African Charter on Human and Peoples' Rights, CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982) (27 June 1981).

¹⁶⁵ For example, the human rights recognized in the Universal Declaration of Human Rights (UN General Assembly resolution 217 A (III) of 10 December 1948) are considered to be reflective of customary international law. See UN, *Proclamation of Teheran, Final Act of the International Conference on Human Rights, Teheran, 22 April to 13 May 1968*, A/CONF.32/41, 3. See also, generally, William A Schabas, *The Customary International Law of Human Rights* (OUP 2021).



cyberspace. For example, during the COVID-19 pandemic, cyber and influence operations targeted the healthcare sector, jeopardizing efforts to safeguard patients' lives and health.¹⁶⁶ Likewise, the dissemination of hate speech online may not only constitute unlawful discrimination against individuals but also fuel violence, especially in fragile settings.¹⁶⁷ And the online moderation of such content has been done by individuals working in dire conditions.¹⁶⁸

However, the obligations enshrined in most human rights treaties apply only within a **State's jurisdiction**; that is, within the scope of application of each treaty.¹⁶⁹ There is no question that States have human rights jurisdiction in their territory: jurisdiction is primarily territorial. But the extent to which such jurisdiction extends extraterritorially is controversial. This question is crucial in the cyber context because a significant number of cyber operations are carried out from ICT infrastructure located in different States and may remotely affect the human rights of individuals in the origin, transit and target States. For example, electronic surveillance might be carried out using cables and servers located in multiple territories and can undermine the privacy of individuals across international borders. Although some States contest the extraterritorial application of human rights,¹⁷⁰ the prevailing view is that such obligations can, at least in some circumstances, extend to a State's actions outside its borders.¹⁷¹ Different models or approaches to extraterritorial human rights jurisdiction have been endorsed by different States and human rights bodies,¹⁷² including:

- a. The **spatial model**, whereby human rights obligations apply in areas under the effective control of a State.¹⁷³
- b. The **personal model**, under which human rights obligations arise whenever a State exercises effective control or authority over persons.¹⁷⁴

166 See, for example, US Cybersecurity & Infrastructure Security Agency, 'COVID-19 Exploited by Malicious Cyber Actors' (8 April 2020); Marko Milanovic and Michael Schmitt, 'Cyber attacks and cyber (mis) information operations during a pandemic' (2020) 11(1) *Journal of National Security Law and Policy* 247.

167 Talita Dias, 'Finding Common Ground: The Right to be Free from Incitement to Discrimination, Hostility, and Violence in the Digital Age' (2024) 16(4) *Global Responsibility to Protect* 391, 392.

168 Andrew Arsht and Daniel Etcovitch, 'The Human Cost of Online Content Moderation', *Jolt Digest* (2 March 2018).

169 See, for example, ICCPR, Article 2(1), which uses the formulation 'all individuals within [a State's] territory and subject to its jurisdiction'.

170 See, for example, the views of the US expressed in its national position (2021) and in UN Human Rights Committee, *Consideration of Reports Submitted by State Parties Under Article 40 of the Covenant, Third Periodic Reports of States Parties Due in 2003: United States of America*, CCPR/C/USA/3 (2005), 109–110.

171 See, for example, ICJ, *Legal Consequences Arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, Including East Jerusalem* (Advisory Opinion) (19 July 2024), para 99.

172 For an overview, see Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (OUP 2011); Priya Urs, Talita Dias, Antonio Coco, and Dapo Akande, *The International Law Protections against Cyber Operations Targeting the Healthcare Sector* (ELAC 2023), 170–173.

173 ECtHR, *Banković and others v Belgium and others* (App no 52207/99) (12 December 2001), para 80.

174 ECtHR, *Al-Skeini and others v United Kingdom* (App no 55721/07) (7 July 2011), paras 136–137.



- c. The **functional model**, under which jurisdiction is defined by effective control over the enjoyment of human rights, even if such control is exercised remotely, such as in the case of foreign surveillance.¹⁷⁵

The spatial model is the most limiting one. It stems from the concern that States are unable to respect, protect, or ensure human rights without effective territorial control. In the cyber context, adopting this approach would mean that a State would lack jurisdiction over conduct that takes place in its territory yet remotely affects the rights of individuals in other States, such as electronic surveillance or foreign electoral interference. The personal model goes a step further by expanding the concept of jurisdiction to situations where a State has physical control over persons. It was originally conceived to cover situations of detention during armed conflict, where the responsible State lacks territorial control yet has the capacity to physically violate human rights. However, this model would still exclude most online activity remotely affecting human rights in other States in the absence of physical proximity between perpetrator(s) and victim(s). The functional model is the most expansive one as it focuses on the enjoyment of human rights, whether physical or non-physical. Thus, it covers a wide spectrum of online activity, regardless of physical proximity between perpetrator(s) and victim(s). This model is grounded in the idea that States are not permitted to violate human rights in other States if they cannot do so at home. It also accommodates the rapid pace of technological development and the new ways in which technology may be used to violate human rights.

Jurisdiction is not a precondition to human rights obligations under customary international law. Nevertheless, there is debate about the extraterritorial scope of customary human rights obligations, as well as a State's capacity to fulfil those obligations.¹⁷⁶

175 HRC, *General Comment No 36: Article 6: Right to Life*, CCPR/C/GC/36 (3 September 2019) (*General Comment 36*), paras 21 and 63. See also Sarah H Cleveland, 'Embedded International Law and the Constitution Abroad' (2010) 110 *Columbia Law Review* 225; Yuval Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law' (2013) 7 *The Law and Ethics of Human Rights* 47

176 Ryan Fisher (ed), *Operational Law Handbook* (National Security Law Department, the Judge Advocate General's School, United States Army, 2022), 96.



States have negative and positive human rights obligations online and offline.

Negative obligations require States to respect human rights by not unlawfully interfering with them.¹⁷⁷ Positive obligations require States to protect human rights from unlawful interference by other States and non-State actors as well as to ensure the conditions for the progressive realization of human rights by taking active steps.¹⁷⁸ Positive human rights obligations are obligations of conduct measured by a standard of due diligence: States must make their best efforts to protect and to ensure human rights to the extent of their jurisdiction and capacity to act.¹⁷⁹ In the digital age, it is particularly important to protect human rights from the conduct of non-State actors, including technology companies and cyber criminals. Positive human rights obligations are separate from other due diligence obligations, including those of general applicability discussed above.

The prevalent view currently is that **corporations** do not have *binding* human rights obligations under international law.¹⁸⁰ However, in its national position, Austria advances the view that ‘business enterprises, regardless of their size, industry, operational context and structure, are also *required* to respect human rights’.¹⁸¹ In any event, in line with the UN Guiding Principles on Business and Human Rights, businesses have a *responsibility* to respect human rights, including by exercising due diligence in identifying, preventing, mitigating, and accounting for their human rights impact online and offline.¹⁸²

Absolute rights, such as freedom of opinion and the prohibition of torture, must never be interfered with, including by cyber means. **Qualified rights**, such as privacy and freedom of expression, may be subject to lawful interference. The conditions for such interference are laid down by relevant treaty provisions and customary rules. However, in general, lawful interference with human rights is subject to the following requirements:

177 See, for example, HRC, *General Comment 31*, para 6.

178 HRC, *General Comment 31*, para 8; IACtHR, *Velásquez Rodríguez v Honduras*, (Merits) (Ser C) No 4 (29 July 1988), para 177.

179 See Antonio Coco and Talita de Souza Dias, ‘“Cyber Due Diligence”: A Patchwork of Protective Obligations in International Law’ (2021) 32 *European Journal of International Law* 795.

180 See, for example, common position of the AU (2024), para 56.

181 See the national position of Austria (2024), p. 13. (Emphasis added.)

182 See OHCHR, ‘*Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework*’, (2011), Principles 11 to 15.



- a. **Legality** – limitations must be grounded in accessible laws and are subject to judicial review.
- b. **Legitimacy** – limitations must be made for a legitimate, public policy aim, such as national security or the protection of the rights of others.
- c. **Necessity** – limitations must be the least restrictive means to achieve the legitimate aim.
- d. **Proportionality** – the limitation in question must be commensurate with the importance of the aim sought.¹⁸³

These conditions must be observed by States when carrying out cyber operations and other online measures to protect legitimate aims, such as targeted surveillance of suspected criminals and online safety regulations.

At a time of increasing militarization of cyberspace, it is also important to bear in mind that **IHRL continues to apply during armed conflict alongside IHL**.¹⁸⁴ Whenever the two regimes provide different levels of protection for civilians, such as in the context of targeting, determining which one is more appropriate to the situation can only be done on a case-by-case basis.¹⁸⁵ As a general rule, the closer the conduct is to the battlefield, the more appropriate IHL will be to regulate it, and vice-versa.

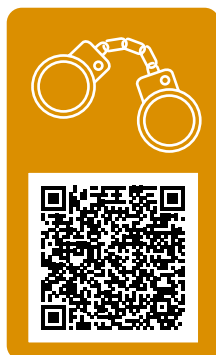
Failure to respect, protect or ensure human rights may give rise to State responsibility. Because human rights are *erga omnes* obligations – obligations owed to all States parties to a treaty or to the international community as a whole – human rights violations may be *invoked* by any State party to the relevant treaty or any State in the case of customary human rights obligations.¹⁸⁶ As discussed below, it remains controversial whether non-victim States may take countermeasures in response to such breaches.

183 HRC, *General Comment 31*, para 6; HRC, *General Comment No 34: Article 19: Freedoms of opinion and expression*, CCPR/C/GC/34 (12 September 2011), paras 21–36.

184 HRC, *General Comment 31*, para 11; ICJ, *Nuclear Weapons Advisory Opinion*, para 25; ICJ, *Wall Advisory Opinion*, paras 105–106; ICJ, *Case Concerning Armed Activities in the Territory of the Congo (Democratic Republic of Congo v Uganda)* (Merits) [2005] ICJ Rep 168, para 216.

185 Cordula Droege, 'Elective affinities? Human rights and humanitarian law' (2008) 90 *International Review of the Red Cross* 501.

186 See ILC, *ARSIWA*, Article 48.



c. International criminal law

Individuals may commit or facilitate international crimes (including the core international crimes of aggression, war crimes, genocide, crimes against humanity) by cyber or non-cyber means. Whether or not a cyber operation amounts to an international crime will depend on the interpretation of the crime and its elements in each case, including the conduct (*actus reus*) and mental elements (*mens rea*), as well as the mode(s) of participation. The core international

crimes are punishable under customary international law and certain treaties, such as the Statute of the International Criminal Court (ICC).¹⁸⁷

Cyber operations amounting to international crimes may be prosecuted

before international and domestic criminal courts with jurisdiction over the alleged offences.¹⁸⁸ This includes the ICC, which has jurisdiction, as a general rule, whenever an element of the crime is committed in the territory or by a national of a State party to the ICC Statute or of a State that has accepted the court's jurisdiction.¹⁸⁹

Cyber operations amounting to international crimes may be prosecuted before domestic or international courts with jurisdiction over the alleged offences.

The use of ICTs to perpetrate or enable international crimes is far from hypothetical. For example, in the context of the war in Ukraine, some cyber operations targeting civilians and civilian infrastructure may not only have amounted to violations of IHL but also war crimes.¹⁹⁰ In 2023, the prosecutor of the ICC announced the development of a policy on the prosecution of 'cyber-enabled crimes', including crimes committed fully by cyber means and cases where cyber operations enable or allow non-cyber conduct that amounts to an international crime.¹⁹¹ At the time of writing, the draft policy has been open for public comments.¹⁹² Nevertheless, to

187 See Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 90 (as amended) ('ICC Statute').

188 See Robert Cryer, Darryl Robinson, and Sergey Vasiliev, *An Introduction to International Criminal Law and Procedure* (CUP 2019), parts II and III.

189 ICC Statute, Article 12(2)-(3).

190 See Lindsay Freeman, 'Ukraine Symposium – Accountability for Cyber War Crimes', *Articles of War* (14 April 2023); Andy Greenberg, 'The Case for War Crimes Charges Against Russia's Sandworm Hackers', *Wired* (12 May 2022).

191 ICC, 'Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system' (22 January 2024).

192 ICC, 'ICC Office of the Prosecutor launches public consultation on policy on cyber-enabled crimes under the Rome Statute' (7 March 2025).



date, only the national position of Austria covers the applicability of ICL in cyberspace.¹⁹³

Most questions arising from the application of ICL to the cyber context will arise in other contexts. For example, proving the intent necessary to convict someone of genocide (the intent to destroy, in whole or in part, a national, religious, ethnic, or racial group a such)¹⁹⁴ can be challenging whether the conduct is carried out online or offline. Likewise, the question of whether conduct is of sufficient gravity to be admissible before the ICC is not exclusive to cyber-enabled conduct.¹⁹⁵ However, some challenges arise specifically from applying ICL to cyber activities.

When interpreting the rules of ICL to assess whether cyber activities constitute or facilitate international crimes, the **principle of legality and its corollaries** (non-retroactivity, strict interpretation, prohibition of analogy, and *in dubio pro reo*) must be respected.¹⁹⁶ This means that the definitions of crimes, the mental element, and the modes of participation cannot be expanded beyond what the text reasonably allows in order to convict individuals for conduct carried out in cyberspace.¹⁹⁷ The principle of legality protects individuals from criminal punishment without fair notice and is a fundamental human right recognized in treaties and customary international law.¹⁹⁸

The interpretation of **war crimes** in the cyber context might also raise specific challenges. War crimes are grave breaches of the Geneva Conventions and other serious violations of IHL.¹⁹⁹ Directing attacks against civilians or civilian objects is a war crime. However, in the ICC's case law, disagreements have emerged about whether conduct may be characterized as an attack by reason of its consequences,²⁰⁰ an issue that is particularly relevant in the cyber context. As noted above, it is also



193 See the national position of Austria (2024), p. 20.

194 Convention on the Prevention and Punishment of the Crime of Genocide (signed 9 December 1948, entered into force 12 January 1951) 78 UNTS 277 (Genocide Convention), Article 2.

195 See ICC Statute, Article 17(1)(d). See also Marco Roscini, 'Gravity in the Statute of the International Criminal Court and Cyber Conduct that Constitutes, Instigates or Facilitates International Crimes' (2019) 30 *Criminal Law Forum* 247.

196 See, for example, ICC Statute, Articles 22-24.

197 See Dapo Akande, 'Sources of International Criminal Law', in Antonio Cassese (ed), *The Oxford Companion to International Criminal Justice* (OUP 2009), 44-45.

198 See, for example, ICCPR, Article 15(1). See also Talita Dias, *Beyond Imperfect Justice: The Principles of Legality and Fair Labelling in International Criminal Law* (Brill 2022); Kenneth S Gallant, *The Principle of Legality in International and Comparative Criminal Law* (CUP 2010).

199 See ICC Statute, Article 8(2).

200 In the context of the ICC, see *Prosecutor v Ntaganda, Appeals Judgment on the appeals of Mr. Bosco Ntaganda and the Prosecutor against the decision of Trial Chamber VI of 8 July 2019 entitled 'Judgment'* (30 March 2021), ICC-01/04-02/06-2666-Red 30-03-2021, paras 1164-1166 and Annex I, Separate opinion of Judges Morrison and Hofmanski, ICC-01/04-02/06-2666-Anx1.



unclear whether cyber operations causing non-physical, functional damage can be considered as attacks,²⁰¹ and to what extent their indirect effects can be taken into account.²⁰² Likewise, the controversy around whether civilian data constitutes a civilian object is also relevant to the interpretation of war crimes, as discussed above.²⁰³

Genocide is the commission of potentially destructive acts with the intent to destroy, in whole or in part, a national, religious, ethnical, and racial group as such.²⁰⁴ Only in rare cases will genocide be fully committed by cyber means. Nevertheless, online speech may constitute instigation to genocide or the separate crime of direct and public incitement to genocide.²⁰⁵ However, it is unclear if and to what extent new forms of online expression such as sharing and liking posts may amount to participation in genocide or incitement thereto.



Crimes against humanity are serious violations of human rights committed as part of a widespread or systematic attack against a civilian population.²⁰⁶ They can be carried out or facilitated by cyber means, such surveillance technology.²⁰⁷ While most acts amounting to crimes against humanity require some physical conduct (for example, murder, extermination, and torture), the crimes of persecution and ‘other inhumane acts’ can be committed fully by cyber means.



201 Compare, for example, the national positions of [Denmark \(2023\)](#), p. 455 and [Israel \(2021\)](#), p. 400 which consider that only physical damage can constitute an attack, with the national positions of [Austria \(2024\)](#), p. 17, [Colombia \(2025\)](#), p. 13, [Costa Rica \(2023\)](#), para 49, [France \(2019\)](#), p. 13, [Germany \(2021\)](#), p. 8, [Japan \(2021\)](#), p. 7, and [New Zealand \(2020\)](#), para 25, which consider that cyber operations may qualify as an ‘attack’ without causing physical damage if they disable the functionality of the target. See also Permanent Mission of Lichtenstein to the United Nations, *The Council of Advisers’ Report on the Application of the Rome Statute to Cyberwarfare* (August 2021), para 12, in the context of war crimes under the ICC Statute.

202 Compare, for example, the national position of the [UK \(2021\)](#), para 24, with ICRC, *IHL and challenges of armed conflicts* (October 2015), 41

203 Compare, for example, the national positions of [Austria \(2024\)](#), p. 18, [Colombia \(2025\)](#), p. 18, [Costa Rica \(2023\)](#), para 50, [Finland \(2020\)](#), p. 7, [Germany \(2021\)](#), p. 8, and [Romania \(2021\)](#), p. 78, which consider that the protection of civilian objects extends to civilian data, with the national positions of [Denmark \(2023\)](#), p. 455 and [Israel \(2021\)](#), p. 401, which state that data cannot be considered an object under IHL.

204 See Genocide Convention, Article 2 and ICC Statute, Article 6.

205 See Genocide Convention, Article 3(c) and ICC Statute, Article 25(3)(b) and (e).

206 See, for example, ICC Statute, Article 7 and ILC, *Draft articles on Prevention and Punishment of Crimes Against Humanity* (2019), Article 1.

207 For example, European Centre for Constitutional and Human Rights, ‘[Surveillance in Syria: European firms may be aiding and abetting crimes against humanity](#)’.



The **crime of aggression** is a *serious* breach of the prohibition of the use of force committed by an individual in a leadership position. In the ICC Statute, an act of aggression must also, by its character, gravity, and scale, constitute a *manifest* violation of the UN Charter.²⁰⁸ As discussed above, some cyber operations may amount to a prohibited use of force if their scale and effects are comparable to the use of armed force, such as when they result in loss or life or physical destruction. However, given the narrower definition of the crime of aggression and the application of the principle of legality, only the gravest and clearly unlawful cyber operations will amount to this crime.



International crimes may be committed through different **forms of participation**.²⁰⁹ Joint perpetration, aiding and abetting, and command responsibility are particularly relevant in cyberspace since cyber conduct will more likely *contribute* to the commission of an international crime by non-cyber means, as opposed to by itself constituting such a crime. An important question arising in the cyber context relates to causation: to what extent can the indirect or reverberating effects of cyber operations be said to be caused by the individual conduct in question? Individual criminal responsibility will likely arise if those effects are intended. But causation becomes crucial when the individual may be convicted on the basis of reckless or negligent behaviour. Many cyber operations potentially causing catastrophic consequences will be averted by advances in cybersecurity, and in those cases the cyber operation may constitute an attempted international crime where the conduct is intentional.²¹⁰

208 See ICC Statute, Article 8 *bis*.

209 See ICC Statute, Articles 25 and 28.

210 See ICC Statute, Article 25(3)(f).

4. State responsibility

This section examines how the law of State responsibility applies to cyber activities. Broadly speaking, this body of law governs the accountability of States for internationally wrongful acts and the legal consequences that flow from such acts. Although it has not been codified in a binding treaty, the ILC's *Articles on Responsibility of States for Internationally Wrongful Acts* (2001) are widely regarded as reflective of customary international law. There is broad consensus that these rules apply in the cyber context,²¹¹ but some States have noted that their application may not always be straightforward due to the unique characteristics of ICTs.²¹² This section examines three key topics that have garnered the most attention in the cyber context: attribution, countermeasures, and the plea of necessity. It highlights areas of general agreement as well as aspects that remain unsettled or contested.



a. Attribution

Attribution is one of the constitutive elements of State responsibility, referring to a legally defined link between a given action (or omission) and a State.²¹³ When the relevant criteria are met, the conduct in question is considered to be attributable to the State, meaning that the law treats it as the State's own conduct. If such attributable conduct breaches an applicable legal obligation binding on the State, it constitutes an internationally wrongful act for which the State is

legally responsible.²¹⁴

As a rule, the conduct of State organs is attributable to the State,²¹⁵ while the actions of non-State actors are not, except under specific conditions.²¹⁶

211 See, for example, the national positions of Australia (2021), p. 5, Austria (2024), p. 8, Canada (2022), para 32, Colombia (2025), p. 14, Czechia (2024), para 52, Denmark (2023), p. 452, Estonia (2019 and 2021, p. 28), Finland (2020), p. 5, Italy (2021), pp. 5-6, Norway (2021), p. 6, Sweden (2022), p. 5, Switzerland (2021), p. 5, and also the common positions of the AU (2024), para 61 and the EU (2024), p. 8. See also *Tallinn Manual 2.0*, 80, para 4.

212 See, for example, the national position of Italy (2021), p. 6; China (2021), Statement on applicability of international law in the OEWG (16 December 2021).

213 ILC, *ARSIWA*, commentary to Article 2, para 12.

214 ILC, *ARSIWA*, Article 2

215 ILC, *ARSIWA*, Article 4.

216 See, in particular, ILC, *ARSIWA*, Article 8.



- **State organs** include entities such as military cyber units, civilian intelligence agencies, law-enforcement officials, and any other entities and individuals that make up the organization of the State. The concept also covers organs placed at the disposal of a State by another State,²¹⁷ such as members of one State's CERT seconded to another State and operating under the receiving State's exclusive authority.²¹⁸ Importantly, the conduct of a State organ is attributable to the relevant State even if the organ exceeds its authority or violates instructions given to it (that is, acts *ultra vires*).²¹⁹
- **Non-State actors'** activities such as cyber operations conducted by individual hacktivists, hacker groups, or ransomware gangs may be attributable to a State under certain conditions. This occurs if they act in complete dependence on the State²²⁰ or act under its instructions, direction, or control.²²¹ The degree of control required remains subject to debate: the ICJ has affirmed that the exercise of 'effective control' is necessary,²²² while the International Criminal Tribunal for the former Yugoslavia developed a less stringent 'overall control' test, applicable to organized groups for the purposes of classifying armed conflict.²²³ Only a few States have taken a view on this issue thus far, and those that have done so all endorsed the effective control test.²²⁴ This appears to be due to a concern that a less stringent test for attribution could lead to abuse. Finally, the conduct of a non-State actor is also attributable to a State if the actor was empowered to exercise elements of governmental authority,²²⁵ or if the State subsequently acknowledges and adopts the conduct as its own.²²⁶

Cyber activities by non-State actors may be attributable to a State when conducted under its control – but the threshold of control required remains contested.

217 ILC, *ARSIWA*, Article 6.

218 *Tallinn Manual 2.0*, commentary to Rule 16, para 4.

219 ILC, *ARSIWA*, Article 7.

220 ICJ, *Nicaragua Case*, para 110; ICJ, *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* (Judgment) [2007] ICJ Rep 43 (*Bosnian Genocide Case*), para 392.

221 ILC, *ARSIWA*, Article 8.

222 ICJ, *Nicaragua Case*, para 115; ICJ, *Bosnian Genocide Case*, para 400.

223 ICTY, *Prosecutor v Tadić* (Appeal Judgment) IT-94-1-A (15 July 1999), paras 116 and ff.

224 See the national positions of *Brazil* (2021), p. 21, *Ireland* (2023), para 22, the *Netherlands* (2019), p. 6, and *Norway* (2021), p. 6.

225 ILC, *ARSIWA*, Article 5.

226 ILC, *ARSIWA*, Article 11.

When a victim State invokes the international responsibility of another State for a cyber activity, this implies that it considers the activity to be attributable to that State. Although international law does not regulate the procedural steps for making such determinations, it is generally accepted that any allegation of a wrongful act should be reasonably substantiated.²²⁷ However, States are not obligated under international law to publicly disclose the evidence on which their attribution is based. This interpretation has been affirmed in several national positions.²²⁸

Even if a cyber activity is not attributable to a State, the State may still bear responsibility in certain exceptional circumstances for its failure to take reasonable measures to prevent, to stop, or to redress the activity. Such responsibility does not arise from the activity itself but from the State's omission to act in accordance with its obligations of due diligence, which have been examined in greater detail above.



b. Countermeasures

Countermeasures are responses to internationally wrongful acts that would otherwise be unlawful but are permitted to induce a State responsible for the wrongdoing to comply with its obligations under international law.²²⁹ They are a circumstance precluding wrongfulness and are well grounded in customary international law.²³⁰ Countermeasures must be distinguished from measures of retorsion, which are unfriendly but lawful acts by the victim State against

the responsible State (such as suspending diplomatic relations).²³¹

227 UN General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/70/174 (22 July 2015), para 28(f); UN 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), para 71.(g). See also, for example, the national positions of [Brazil \(2021\)](#), p. 21, [Germany \(2021\)](#), p. 12, [Russia \(2021\)](#), p. 80, and [Switzerland \(2021\)](#), p. 6.

228 See, for example, the national positions of [Australia \(2021\)](#), p. 5, [Canada \(2022\)](#), para 33, [Czechia \(2024\)](#), para 58, [Denmark \(2023\)](#), p. 452, [Finland \(2020\)](#), p. 6, [France \(2019\)](#), p. 11, [Germany \(2021\)](#), p. 12, [Israel \(2021\)](#), pp. 404-405, [Italy \(2021\)](#), p. 5, [the Netherlands \(2019\)](#), p. 6, [New Zealand \(2020\)](#), para 20, [Sweden \(2022\)](#), p. 5, [Switzerland \(2021\)](#), p. 6, [the UK \(2018 and 2021\)](#), para 15), and the US ([2016](#), p. 19 and [2021](#), p. 141), and also the common position of the [EU \(2024\)](#), p. 8.

229 ILC, *ARSIWA*, Commentary, part 3 ch 2 at para 1.

230 ILC, *ARSIWA*, Article 22, paras 1-2, and Commentary to Chapter II of Part Three, para 1.

231 Elizabeth Zoller, *Peacetime Unilateral Remedies: An Analysis of Countermeasures* (Transnational 1984) 5.



Most States accept the applicability of countermeasures to cyber operations.²³² This is because countermeasures are one of the few avenues with which States can enforce international law in the absence of a global police force.²³³

With the rise in the number and sophistication of wrongful cyber operations, countermeasures are an important accountability tool in cyberspace.

However, at least one State, Brazil, has questioned their customary status generally.²³⁴ This view seems to draw on the objections raised by several developing countries to the inclusion of countermeasures in the ILC Articles on State Responsibility in the early 2000s.²³⁵ Others have condemned recourse to countermeasures in the cyber context out of a concern with conflict escalation and the militarization of cyberspace.²³⁶ The topic is controversial and this is why, for example, it is expressly excluded from the common position of the AU.²³⁷

To ensure that countermeasures are not subject to abuse, strict **substantive and procedural conditions** apply to them under general international law. Notably, countermeasures must be aimed solely at inducing compliance, targeted at the responsible State, proportionate to the injury suffered, temporary and reversible as far as possible in their effects, and consistent with certain international obligations such as the prohibition of the use of force and respect for fundamental human rights.²³⁸ But countermeasures need not be in kind; in other words, international law does not preclude the use of cyber countermeasures to respond to a non-cyber internationally wrongful act, and vice versa. Furthermore, before taking countermeasures the victim State must make a prior demand by calling the responsible State to comply with its international obligations. As a general rule, the victim

232 See, for example, the national positions of Australia (2021), p. 5, Austria (2024), p. 8, Canada (2022), para 34, Costa Rica (2023), para 13, Denmark (2023), p. 453, Estonia (2019 and 2021, p. 28), Finland (2020), p. 5, France (2019), p. 8, Germany (2021), p. 13, Ireland (2023), para 25, Israel (2021), p. 405, Italy (2021), p. 7, Japan (2021), p. 4, the Netherlands (2019), p. 7, New Zealand (2020), para 21, Norway (2021), p. 8, Poland (2022), p. 7, Romania (2021), p. 79, Russia (2021), p. 80, Singapore (2021), p. 84, Sweden (2022), p. 6, Switzerland (2021), p. 6, the UK (2018, 2021, para 17, and 2022), and the US (2016, p. 20, 2020, 2021, p. 142), and also the common position of the EU (2024), p. 9.

233 ILC, *ARSIWA*, Commentary, Chapter II of Part Three, para 1.

234 See the national position of Brazil (2021), p. 21.

235 See, for example, UN General Assembly, *Report of the International Law Commission on the work of its fifty-second session*, A/CN.4/513 (15 February 2001), para 149, reflecting concerns that countermeasures 'favoured more powerful States' to the detriment of 'small and weak States'.

236 See the national positions of China (2021), p. 1 and Cuba (2024) para 8.

237 See the common position of the AU (2024), para 10.

238 ILC, *ARSIWA*, Articles 49–51.

State must also notify the responsible State and offer to negotiate with it before resorting to countermeasures, unless urgency requires immediate action; for example, to preserve its rights.²³⁹ Countermeasures may be taken when negotiations are ongoing, or a dispute is pending before a dispute settlement body. But they must be suspended if the dispute settlement body has the power to issue binding decisions ordering equivalent measures and the prior breach has ceased.²⁴⁰

There is some debate about how these general conditions apply in the cyber context. For example, some States have argued in their national positions that the requirement of prior demand may be dispensed with in urgent cases.²⁴¹ Underlying this view is the concern that, by making a prior demand, the victim State might lose the element of surprise or reveal sensitive cyber capabilities.²⁴²

The notion of **collective countermeasures** – countermeasures taken by States other than the victim State – remains contentious, especially in cyberspace.²⁴³ Inconsistent use of the term compounds the uncertainty around the issue. The debate about whether collective countermeasures are lawful has gained particular traction given the formation of cyber alliances and joint responses to malicious cyber operations.²⁴⁴ Some States have expressed their support for the taking of countermeasures in the general interest; that is, in response to breaches of *erga omnes* obligations, such as those protecting human rights.²⁴⁵ A smaller number of States have also supported the taking of countermeasures on behalf of victim third States, irrespective of the type of obligation breached.²⁴⁶ Support for collective countermeasures is grounded in the idea of international solidarity and that of the protection of human rights and other collective values. Collective countermeasures could also address asymmetries in cyber capabilities by allowing more capable States to take measures on behalf of smaller ones. However, other States have rejected the permissibility

239 ILC, *ARSIWA*, Article 52(1)-(2).

240 ILC, *ARSIWA*, Article 52(3).

241 See the national positions of *Costa Rica* (2023), para 14, *Italy* (2021), p. 7, *Switzerland* (2021), p. 6, the *UK* (2018 and 2021, para 19), and the *US* (2016, p. 22, 2020, and 2021, p. 142).

242 See Henning Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (CUP 2020), 138.

243 See Talita Dias, *Countermeasures in international law and their role in cyberspace* (Chatham House 2024) 33–54.

244 See, for example, Ashley Deeks, 'Defend Forward and Cyber Countermeasures', Hoover Working Group on National Security, Technology, and Law (2020), 8–9; Michael N Schmitt and Sean Watts, 'Collective cyber countermeasures?' (2021) 12 *Harvard National Security Journal* 373.

245 See, for example, the national positions of *Austria* (2024), p. 9, *Colombia* (2025), p. 17, *Ireland* (2023), paras 25–26, and *Poland* (2022), p. 8.

246 See, for example, the national positions of *Costa Rica* (2023), para 15, and *Estonia* (2019).



of collective countermeasures under international law.²⁴⁷ Concerns with a cyber arms race, disproportionate effects, conflict escalation, and the destabilization of treaty relations seem to underlie those views.²⁴⁸ The stance that States have taken on collective countermeasures in other contexts, such as the war in Ukraine, may also determine their views in the cyber context.²⁴⁹

Finally, some States have suggested that third States may aid or assist a victim State in the taking of its countermeasures, including in the cyber context.²⁵⁰ This view is based on the understanding that the victim State is acting lawfully and that the assisting State likewise incurs no international responsibility, provided that its assistance – which may include measures such as the provision of funds, intelligence, training, or equipment – is itself lawful under international law.²⁵¹



c. Necessity

Like countermeasures, the plea of necessity is a circumstance precluding the wrongfulness of conduct that would otherwise be inconsistent with a State's international obligations. Most States agree that necessity is grounded in customary international law and the ICJ has recognized as much.²⁵² But this is an exceptional defence in that it is only available where there is a **grave and imminent peril against the essential interests** of a State, its people, or the international community.²⁵³ Even under these circumstances, the State's action must not seriously impair the essential interests of the affected State(s) or the international community.²⁵⁴ This means that the impact of the acts justified by the plea of necessity must not be greater than the harm being

247 See, for example, the national positions of [Canada \(2022\)](#), para 37, and [France \(2021\)](#), p. 4

248 See, for example, UN General Assembly, *Sixth Committee, Summary record of the 15th meeting*, A/C.6/55/SR.15 (13 November 2000), para 25 (Israel); UN General Assembly, *Sixth Committee, Summary record of the 14th meeting*, A/C.6/55/SR.14 (10 November 2000), para 31 (UK); and China, 'Statement by the Chinese Delegation at the Thematic Debate of the First Committee of the 72th UNGA' (2017).

249 See for example, Council of the EU (2023), 'EU sanctions – New recital in Council Decision', (CFSP) 2023/191 of 27 January 2023 – Countermeasures, WK 5169/2023 INIT, para 4; Italy, Regional Administrative Tribunal for Lazio (Second Session), N. 08669/2022 REG.PROV.COLL, N. 04902/2022 REG.RIC., [Sentence](#) (2022).

250 See, for example, the national positions of [Canada \(2022\)](#), para 37, and [Denmark \(2023\)](#), p. 454.

251 ILC, *ARSIWA*, Commentary to Article 16, paras 5–6; Talita Dias, *Countermeasures in international law and their role in cyberspace* (Chatham House 2024) 50–54; Miles Jackson and Federica Paddeu, 'The Countermeasures of Others' (2024) 118(2) *American Journal of International Law* 231, 254–255.

252 See ILC, *ARSIWA*, Commentary to Article 25, para 14; ICJ, *Gabčíkovo-Nagymaros Project (Hungary/Slovakia)* (Judgment) [1997] ICJ Rep 7, para 51.

253 ILC, *ARSIWA*, Article 25(1)(a) and Commentary, para 15.

254 ILC, *ARSIWA*, Article 25(1)(b).



averted.²⁵⁵ Moreover, the plea of necessity is not available to States that have substantially contributed to the situation in which they find themselves or when the international obligation in question excludes the defence.²⁵⁶ For example, necessity cannot justify breaches of the prohibition of the use of force, which has its own exceptions.²⁵⁷

Several States have recognized the applicability of necessity in the cyber context in their national positions.²⁵⁸ Necessity has also been floated as a possible justification for defensive cyber operations against ongoing or impending harms, often called 'active cyber defence' or 'defend forward'.²⁵⁹

Unlike countermeasures, **the plea of necessity can be asserted even where there is no violation of international law by a State.** This means that the defence is not dependent on attribution and is available as a response to the acts of non-State actors. And necessity can justify actions that would otherwise violate the rights of non-responsible States if the above conditions are met. Moreover, necessity does not depend on actual damage and may be invoked preventively against imminent threats. As noted by the Netherlands in its national position, necessity 'is primarily aimed at giving a State the opportunity to protect its own interests and minimise the damage it suffers'.²⁶⁰

These features make the plea of necessity particularly attractive in the cyber context, given the attribution challenges discussed above. However, States have stressed the exceptional nature of the defence and the very

Unlike countermeasures, the plea of necessity can be invoked even without a prior wrongful act by another State, making it attractive in the cyber context where attribution is often uncertain.

stringent conditions to which it is subject. This is to avoid abuse and the risk of conflict escalation, which could be especially high in cyberspace's fast-paced and interconnected environment.

255 ILC, *ARSIWA*, Commentary to Article 25, paras 1 and 17.

256 ILC, *ARSIWA*, Article 25(2).

257 ILC, *ARSIWA*, Commentary to Article 25, para 21.

258 See the national positions of *Costa Rica (2023)*, para 16, *Czechia (2024)*, para 61, *France (2019)*, p. 8, *Germany (2021)*, p. 14, *Japan (2021)*, p. 5, the *Netherlands (2019)*, pp. 7-8, *Norway (2021)*, p. 9, *Sweden (2022)*, p. 6, *Switzerland (2021)*, p. 7, and also the common position of the *EU (2024)*, p. 9.

259 See 'Applying the Plea of Necessity to Cyber Operations', Meeting Summary, Chatham House, International Law Programme (27 September 2023); Henning Lahmann, 'The Plea of Necessity in Cyber Emergencies' (2023) 92 *Nordic Journal of International Law* 422.

260 National position of the *Netherlands (2019)*, p. 8.



It has been noted that necessity is **available as a response to physical and non-physical harms**.²⁶¹ In their national positions, some States have proposed the following examples of cyber operations that could amount to a 'grave and imminent peril' to an 'essential interest' and therefore trigger the plea of necessity: an internet shutdown²⁶² and a cyber operation targeting critical infrastructure,²⁶³ such as a nuclear power plant.²⁶⁴ Imminence, in this context, not only means temporally proximate perils but also those that are certain or inevitable.²⁶⁵

5. Conclusion

This chapter has provided an overview of the key substantive legal issues relevant to the preparation of national positions on the application of international law to cyber activities. Their selection was guided by the positions published so far, ongoing multilateral discussions at the OEWG, and the closed-door consultations organized in the context of this project.

The chapter was structured around three broad categories. First, it began with foundational principles of international law, including sovereignty, non-intervention, the prohibition of the use of force, due diligence, the peaceful settlement of disputes, and self-determination. Second, it considered the applicability and interpretation of three specialized regimes of international law: IHL, IHRL, and ICL. Third, it looked at the law of State responsibility, with a focus on attribution, countermeasures, and the plea of necessity.

Across these areas, the analysis revealed important points of convergence and divergence among States. States agree that international law is applicable to the use of ICTs in general and in relation to the specific regimes explored in this chapter. They also often agree on the elements of the applicable rules (for example, that an act must bear on matters within a State's internal or external affairs and be coercive in nature to constitute a prohibited intervention). And sometimes there is agreement that an issue, like due diligence, requires further study.

²⁶¹ See, for example, the national positions of [Czechia \(2024\)](#), para 68, [Germany \(2021\)](#), p. 15 and the [Netherlands \(2019\)](#), p. 8.

²⁶² National position of the [Netherlands \(2019\)](#), p. 8.

²⁶³ National position of [Germany \(2021\)](#), pp. 14-15.

²⁶⁴ See 'Applying the Plea of Necessity to Cyber Operations', Meeting Summary, Chatham House, International Law Programme (27 September 2023), para 5.

²⁶⁵ ICJ, [Gabčíkovo-Nagymaros Project \(Hungary/Slovakia\)](#) (Judgment) [1997] ICJ Rep 7, para 54.



At the same time, important differences remain. These include questions of whether a certain legal standard constitutes a standalone rule in the cyber context (as is the case with sovereignty and due diligence), what is the threshold at which a cyber operation qualifies as a violation of the rule in question (for example, sovereignty and the prohibitions of intervention and use of force), and how to qualify a category of conduct carried out by cyber means (such as cyber espionage). These divergences serve as an incentive for States to continue developing their views and contribute to ongoing debates.

For States developing national positions, the overview in this chapter thus provides a roadmap for selecting issues or topics to include (or to avoid), navigating the points of contention, forming their views on those various issues, and ultimately finding common understandings on how international law applies in the cyber context. Once these substantive questions have been addressed, the next step is to decide how a national position should be presented, including its format, style, language, and dissemination strategies. This is what the following chapter turns to.




































		Common positions		National positions																																			
																																							
		AU	EU	AU	AT	BR	CA	CN	CO	CR	CU	CZ	DK	EE	FI	FR	DE	IR	IE	IL	IT	JP	KZ	KE	NL	NZ	NO	PK	PL	RO	RU	SG	SE	CH	UK	US			
Foundational rules and principles	Sovereignty	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			
	Non-intervention	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			●	●	●	●	●	●	●	●	●	●	●	●	●		
	Use of force	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			●	●	●	●	●	●	●	●	●	●	●	●	●		
	Due diligence	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●		●	●	●	●			●	●	●		●	●			●	●	●	●	●	
	Peaceful settlement of disputes	●	●	●	●	●	●	●	●	●	●	●		●		●						●		●		●	●	●				●	●		●	●	●	●	
	Self-determination																		●		●										●								
Specialized regimes	IHL	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●		●	●	●	●		●	●	●	●	●	●	●		●	●	●	●	●	●	●	
	IHRL	●	●	●	●	●	●		●	●		●	●	●	●				●		●	●	●	●	●	●	●		●	●		●	●	●	●	●	●	●	
	ICL				●																																		
State responsibility	Attribution	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●		●	●	●	●			●	●	●		●	●	●		●	●	●	●	●	●	●
	Countermeasures		●	●	●	●	●		●	●		●	●	●	●	●	●		●	●	●	●			●	●	●		●	●	●		●	●	●	●	●	●	●
	Necessity		●		●					●		●			●	●	●					●			●		●						●	●					

Figure 8: Overview of common and national positions by topics covered.



CHAPTER 5:

PRESENTATION



5



AT A GLANCE

This chapter explores how States can present and disseminate their national positions. It compares written and oral formats, discusses length, structure, language, and use of examples, and outlines options for dissemination. Each choice will affect a position's clarity, reach, and impact. The chapter encourages States to balance legal authority with accessibility and to tailor their approach to their objectives, audiences, and available resources.

1. Introduction

Though the national positions issued so far cover a fairly consistent list of topics, as discussed in **Chapter 4**, they have been presented in a variety of ways. The first ones were delivered as government speeches, but the trend has gradually shifted to publishing them as standalone written documents. National positions also vary significantly in length, ranging from concise documents of just a couple of pages to more detailed papers spanning over 20 pages. Some are very general, while others delve deeper into difficult questions of international law and/or specific challenges arising in cyberspace, including scenarios or examples of malicious cyber operations. The structure of positions also varies, with some employing clear headings, numbered paragraphs, and/or summaries. Most national positions have been published in English, with some also published in or translated to other languages. National positions have been disseminated to various audiences using different strategies, including press releases, cross-publications in academic journals or blogs, social media announcements, and events to discuss their content.

The presentation of a national position is not merely a reflection of domestic or regional idiosyncrasies; it also largely determines what its impact will be. The purpose of this chapter is to unpack the various trends in the format, style, language, and dissemination of national positions. This chapter also considers why these choices matter and what their implications are for the status, content, and impact of national positions.

As discussed in the **Introduction** to this Handbook, we consider a national position to be a public statement, published in written form, that lays out the views of a State on one or more substantive questions regarding the application of international law in the cyber context.



That is not to say that States have not expressed their views on various aspects of how international law applies in the cyber context in other formats. For example, many States have made oral remarks and/or submitted written statements at the UN Open-Ended Working Group (OEWG) on questions of international law that they think should be included in its annual reports.¹ Among them are several Global South countries that have yet to publish a national position, such as Chile,² South Africa,³ and certain member States of the Pacific Islands Forum.⁴ These statements can in fact serve as the backbone or starting point for a fully-fledged national position. However, insofar as they do not articulate the substantive views of a State on how different rules and principles of international law apply to cyber activities, they fall outside the scope of this Handbook – as discussed below, so far, only three States have used their statements at the OEWG to present their national positions.

Some policy choices will shape the format, style, language, and dissemination strategies of national positions.

This includes, above all, the choice of legal status of the national position; that is, whether it constitutes evidence of State practice and/or *opinio juris*, an interpretative aid, or a mere political declaration. Second, as discussed in **Chapter 3**, it is important to consider whether the position will follow a deductive approach to international law (by stating relevant rules in the abstract and then explaining how they apply in the cyber context) or the inductive approach (by starting from specific factual challenges in the cyber context and then unpacking which rules apply). Third, the functions, aims and/or motivations of a national position will also inform choices in format, style, language, and dissemination. As seen in **Chapter 2**, the overarching functions of a national position might include to communicate or to engage with different stakeholders, to transform or to adapt international law as it applies to cyber activities, and to prevent unlawful behaviour. This might translate into specific aims and motivations, including preventing miscalculations and escalations by increasing predictability and stability at scale, enhancing compliance and accountability, and shaping the evolution of international law by addressing legal uncertainty.

1 See, for example, Austria, *Pre-Draft Report of the OEWG – ICT: Comments by Austria* (31 March 2020).

2 Ministry of Exterior Relations of Chile, *Derecho Internacional*, UN, New York, OEWG, Sixth Substantive Session (11-15 December 2023).

3 See South Africa, *Statement by South Africa in the ninth session of the Open-Ended Working Group on security of and in the use of ICTs (2021-2025) - International Law*, UN, New York (4 December 2024).

4 Pacific Islands Forum, *Statement delivered by PIF Chair on behalf of the Pacific Islands Forum*, UN (New York, 4 December 2024).



2. Format and style

For the purposes of this chapter, a national position's format and style encompasses its form (oral vs written), its length (long vs concise), and other structural elements such as the use of examples or case studies, summaries, headings, references, numbered paragraphs, and visual aids.

a. Oral vs written form

i. Speeches

The concept of a national position emerged when the legal advisor to the US Department of State, Harold Hongju Koh, articulated the country's views on international law in cyberspace in a speech at the Cyber Command's Inter-Agency Legal Conference in 2012. The speech was published and became a reference point for how the US positioned itself on how different rules and principles of international law applied to information and communications technologies (ICTs).⁵ It was delivered against the background of seminal discussions on this topic that primarily took place within the 2009-2010 and 2012-2013 UN Group of Governmental Experts (GGE)⁶ as well as during the process leading to the publication of the first edition of the *Tallinn Manual* in 2013.⁷ In two further speeches in 2016⁸ and 2020,⁹ the US covered more specific topics or areas of international law that had been discussed at the 2014-2015 GGE, including sovereignty, international humanitarian law (IHL), non-intervention, and international human rights law (IHRL).¹⁰

5 National position of the US (2012).

6 See UN 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/65/201 (30 July 2010), paras 14 and 16; UN General Assembly, *Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General*, A/66/152, A/66/152 (15 July 2011), 6, 18-19; UN 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), paras 11, 16 and 19. See also Eneken Tikk-Ringas, *Developments in the Field of Information and telecommunication in the context of international security: Work of the UN first Committee 1998-2012*, ICT4Peace (2012), 9-10; Camino Kavanagh, *The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century*, UNIDIR (2017), p16-19.

7 See CCDCOE, *The Tallinn Manual*; Wikipedia, 'Tallinn Manual'.

8 National position of the US (2016).

9 National position of the US (2020).

10 UN 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), para 28.



In 2016, Norbert Riedel, the commissioner for international cyber policy in Germany's Federal Foreign Office, delivered a speech on 'Cyber Security as a Dimension of Security Policy' at Chatham House.¹¹ Though not focussed on international law, the speech briefly discussed how, in Germany's view, sovereignty, the prohibition of the use of force, and IHL should be understood in the cyber context. The speech was not framed as Germany's national position, which was published as a standalone written document in 2021, but provided the basis for it.¹²

In 2018, also at Chatham House, the UK attorney general, Jeremy Wright, delivered the country's first national position as a speech titled 'Cyber and International Law in the 21st Century'.¹³ This was repeated for the UK's national position in 2022.¹⁴ In 2019, President Kersti Kaljulaid unveiled Estonia's first national position as a speech at the opening of NATO's flagship cyber conflict conference, 'CyCon'.¹⁵ Israel followed suit in 2020 with a speech delivered by its deputy attorney general, Roy Schöndorf, at the US Naval War College. The speech was published as an academic article¹⁶ and a blog post.¹⁷

11 Federal Foreign Office of Germany, "'Cyber Security as a Dimension of Security Policy". Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London' (18 May 2015).

12 National position of Germany (2021).

13 National position of the UK (2018).

14 National position of the UK (2022).

15 National position of Estonia (2019), pp. 23-30.

16 Roy Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) *International Law Studies*, 97, pp. 395-406.

17 Roy Schöndorf, 'Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', *EJIL: Talk!* (9 December 2020).



Releasing a national position as an official government speech can be an effective way to get the attention of target audiences and to bring more publicity to the document.

There is usually a certain degree of ceremony surrounding the delivery of an official speech, especially one by a high-profile State representative such as a president or attorney general. Because a government speech can bring different stakeholders together, it can also be a good opportunity for questions and feedback. Speeches tend to be less formal and more concise, accessible, and memorable, connecting more closely with audiences. In this way, they can enhance a national position's reach and impact among different stakeholders. On the other hand, their less structured format can be harder to follow, especially for non-lawyers. There is also a risk of creating an expectation that new or follow-up speeches on international law in cyberspace will be delivered. Likewise, the oral form naturally limits the breadth and depth of a national position: there are only so many topics or issues that can be dealt in a single speech, and at a very general level at best.

ii. UN statements

Some States – Brazil,¹⁸ Czechia,¹⁹ and Finland²⁰ – shared their views on international law and cyber activities in oral statements before the OEWG's second substantive session in 2020. In the case of Finland, though the oral statement was never published, it was followed by a longer submission that became the country's standalone written national position.²¹ States have limited time to read their statements during OEWG sessions (usually 3-5 minutes). Therefore, these statements cover a narrower range of topics and are more concise and general in style. However, the UN setting requires a more formal tone than other institutional environments, such as conferences or universities.

Like speeches, **UN statements can be a good way to get the attention of UN member States and stakeholders attending or following the relevant OEWG session.** However, if transcripts are not published and made easily accessible, the risk is that audiences who were not attending or following the relevant meeting – including other States – will not be aware of or have easy access to the content of the statements. For this reason, this Handbook does not consider unpublished or inaccessible statements as national positions.

18 National position of [Brazil \(2020\)](#).

19 National position of [Czechia \(2020\)](#).

20 See Marja Lehto, 'Finland's views on International Law and Cyberspace' (2023), *Nordic Journal of International Law* 92(3), 456–469, and Michael Schmitt, 'Finland Sets Out Key Positions on International Cyber Law', *Just Security* (27 October 2020).

21 National position of [Finland \(2020\)](#).



iii. Standalone written documents

As more areas or topics of international law in cyberspace were being discussed in different forums, including at the UN and in academia, States started to consider issuing national positions as standalone written documents. The first to do so was Australia in 2017, which published its national position as an annex to its International Cyber Engagement Strategy.²² It was followed by France²³ and the Netherlands in 2019.²⁴ France's national position was published by its Ministry of Armed Forces whereas the Netherlands' position was a letter to its parliament. Iran, Finland, and New Zealand published standalone national positions in 2020.²⁵

It was against this background of increasing publications of national positions that the GGE in 2019 invited States to submit 'voluntary national contributions on the subject of how international law applies to the use of information and communications technologies'.²⁶ The idea was for more States to issue a written national position consolidating their views on how international law applies to cyber activities in one single document. The aim was to enhance transparency, predictability, and mutual understandings on the matter. Fifteen States responded to the GGE's call and their positions were published in a GGE Official Compendium in 2021.²⁷ They were Australia, Brazil, Estonia, Germany, Japan, Kazakhstan, Kenya, the Netherlands (which submitted a copy of its 2019 national position), Norway, Romania, Russia, Singapore, Switzerland, the UK, and the US.

Following the publication of the GGE Official Compendium, several other States published their national position as a standalone document. Italy did so in 2021.²⁸ And in the same year France published an English version of its 2019 position.²⁹ Also in 2021, China published two position papers: a more general one on 'International Rules-making in Cyberspace'³⁰ and one on the 'Application of the Principle of Sovereignty in Cyberspace'.³¹

22 National position of [Australia](#) (2017).

23 National position of [France](#) (2019).

24 National position of the [Netherlands](#) (2019).

25 National positions of [Iran](#) (2020), [Finland](#) (2020) and [New Zealand](#) (2020).

26 UN General Assembly, *Resolution adopted by the General Assembly on 22 December 2018 [on the report of the First Committee (A/73/505)] 73/266. Advancing responsible State behaviour in cyberspace in the context of international security*, A/RES/73/266 (2 January 2019), para 3.

27 UN 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 submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266*, A/76/136* (13 July 2021).

28 National position of [Italy](#) (2021).

29 National position of [France](#) (English version) (2021).

30 National position of [China](#) (general) (2021).

31 National position of [China](#) (sovereignty) (2021).

Canada, Poland, and Sweden published their national positions in 2022;³² Costa Rica, Denmark, Ireland, and Pakistan in 2023;³³ Austria, Cuba, and Czechia in 2024;³⁴ and Colombia in 2025.³⁵ The AU and the EU published common positions in 2024.³⁶

Standalone written documents have become the most popular format for publishing national positions. They allow for greater coverage and detail, making them ideal for States seeking to issue more comprehensive and influential positions. The process for publishing a standalone written position also tends to be more formal than that for issuing speeches, statements, or academic articles. There is also an expectation that standalone written positions will become the reference point for a State's views on international law in cyberspace, meaning that the stakes are usually higher with this format. All of this means that the drafting of a standalone written position might take longer and involve more government stakeholders than the drafting of a speech, statement, or academic article. On the one hand, this allows for a more refined and representative national position. On the other, it might lead to more complex documents, which can reduce their accessibility to non-specialist audiences.

iv. Academic articles

As noted above, the 2016 national position of the US was originally issued as a speech that was published the following year as an academic article, in the *Berkeley Journal of International Law*.³⁷ Israel did the same, publishing the speech delivered by its deputy attorney general as an academic article in *International Law Studies* in 2021.³⁸ In 2023, the *Nordic Journal of International Law* published a special issue that contained the previously published national positions of Finland, Norway, and Sweden, while unveiling the national position of Denmark, all with introductions written by the responsible legal advisors.³⁹

32 National positions of [Canada \(2022\)](#), [Poland \(2022\)](#), and [Sweden \(2022\)](#).

33 National positions of [Costa Rica \(2023\)](#), [Denmark \(2023\)](#), [Ireland \(2023\)](#), and [Pakistan \(2023\)](#).

34 National positions of [Austria \(2024\)](#), [Cuba \(2024\)](#), and [Czechia \(2024\)](#).

35 National position of [Colombia \(2025\)](#).

36 Common positions of the [AU \(2024\)](#) and the [EU \(2024\)](#).

37 Brian J. Egan, 'International Law and Stability in Cyberspace' (2017) 35 *Berkeley Journal of International Law* 35, 169-180.

38 Roy Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) *International Law Studies*, 97, 395-406.

39 Jeppe Mejer Kjelgaard and Ulf Melgaard, 'Denmark's Position Paper on the Application of International Law in Cyberspace' (2023) *Nordic Journal of International Law*, 92(3), 446-455; Marja Lehto, 'Finland's views on International Law and Cyberspace' (2023), *Nordic Journal of International Law* 92(3), 456-469; Vibeke Musæus, 'Norway's Position Paper on International Law and Cyberspace' (2023) *Nordic Journal of International Law* 92(3), 470-488; Ola Engdahl, 'Sweden's Position Paper on the Application of International Law in Cyberspace' (2023) *Nordic Journal of International Law* 92(3), 489-497.



Publishing national positions as academic articles can bring rigour and legal authority to the publication, given the high standards of peer and/or editorial review that academic articles usually go through. Academic articles can also be an effective way to reach out to and influence specialist legal audiences, especially academics. On the other hand, they might not be easily accessible to non-specialists. This is because of the complex language normally used in academic articles as well as the fact that not many non-specialists are aware of academic publications.

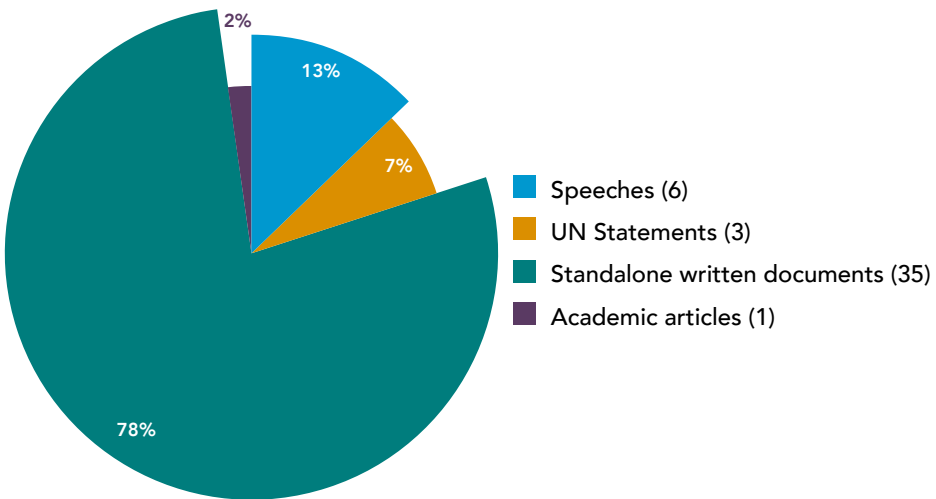


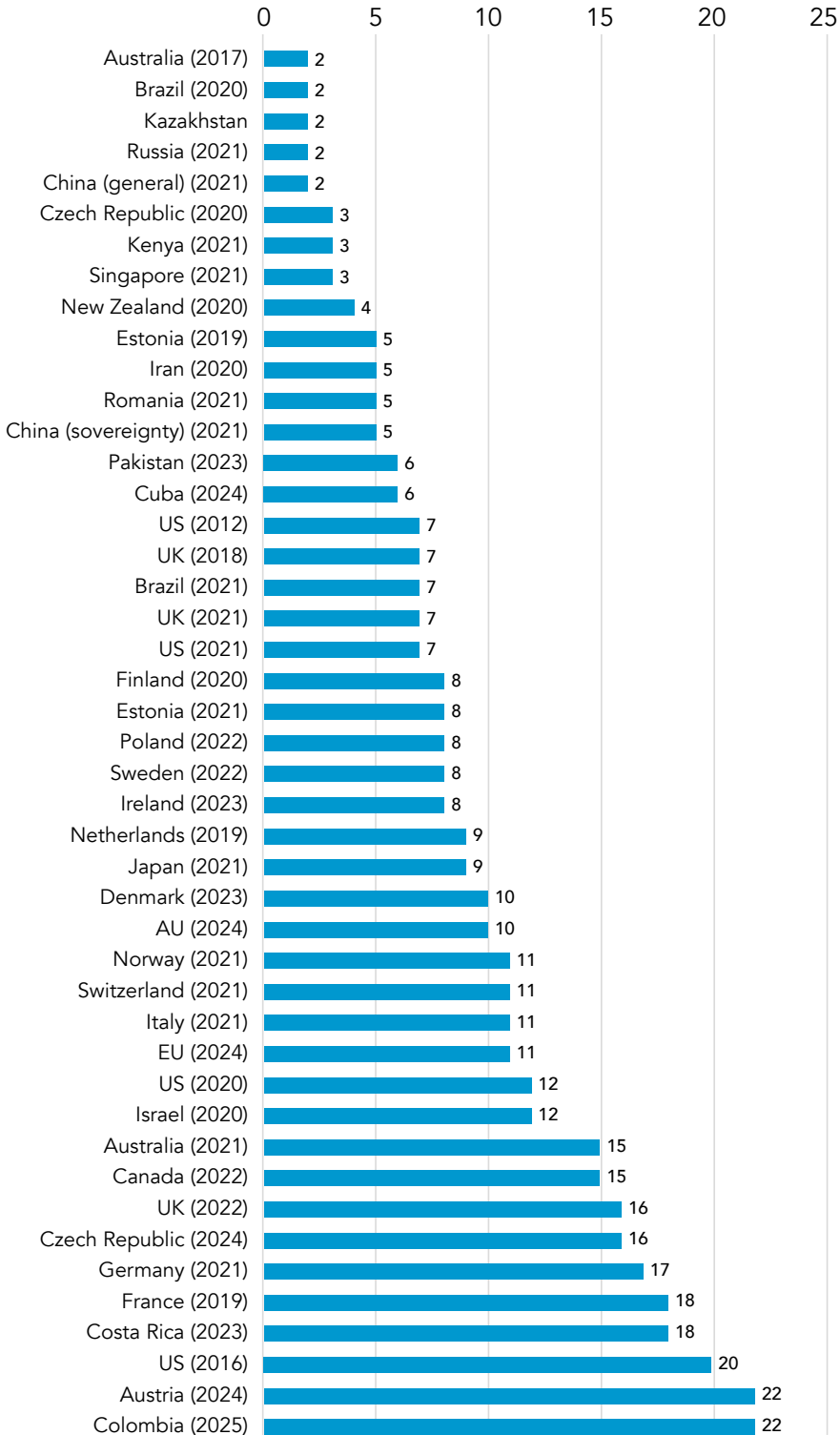
Figure 9: Proportion of oral vs written national and common positions.

b. Length

The length of the national positions published to date varies significantly: the shortest are two-pages long (for example, Australia (2017), Kenya, Kazakhstan, and Russia) while the longest are 22-pages long (Austria and Colombia). However, as the chart below indicates, **there is a preference for longer detailed documents with an average of nine pages**, most of which have been originally published in written form.



Figure 10: National and common positions by length (in pages).





The preference for longer documents can be explained by the breadth and depth of analysis that the standalone format allows. For example, the national positions of Austria and Costa Rica (22 and 18 pages, respectively) have resonated positively among academics, with some welcoming their sophistication, detail, breadth, and nuance.⁴⁰ As discussed in **Chapter 4**, a variety of rules, principles, and regimes may be relevant to cyberspace, and each raises complex questions of legal interpretation and implementation. Therefore, breadth and depth of analysis are particularly important if the national position seeks to develop or clarify existing international law as it applies in the cyber context or to influence academic scholarship. Breadth and depth are also conducive to greater transparency and accountability. At the same time, too much detail and excessive formalism or legalese can impact a national position's clarity and accessibility, particularly for non-legal audiences.

That is not to say that concise national positions have less value. These can be useful if a State intends to focus on a few key areas or topics of international law as they apply in the cyber context.⁴¹ Concise national positions are also appropriate if the aim is to simply acknowledge the general applicability of international law and/or selected rules, principles, or regimes in cyberspace, without delving into the specifics or complexities of how they apply in that context.⁴² Likewise, if the purpose of a national position is to flag areas of uncertainty or gaps, a concise paper might be more suitable. Policy statements on issues such as the cyber threat landscape, capacity-building, or confidence-building also do not require the same level of detail as legal analysis and can be made in a more concise and informal manner.⁴³ Therefore, concise positions can be useful for high-level diplomatic discussions on broader policy issues surrounding the applicability of international law in the cyber context. Relatedly, practitioners tend to prefer shorter documents, given their limited time to study national positions in full. For example, during the project roundtables, the concise format of New Zealand's national position (four pages) was lauded by a State representative as 'elegant' and a model to strive for.⁴⁴ A concise format is also appropriate if the aim of a national position is to inform a broader audience of non-experts in international law, including policymakers, industry, and civil society.

40 See Chris Carpenter and Duncan B. Hollis, 'A Victim's Perspective on International Law in Cyberspace', *Lawfare* (28 August 2023); Przemysław Roguski, 'Austria's Progressive Stance on Cyber Operations and International Law', *Just Security* (25 June 2024).

41 See, for example, the national position of Estonia (2019).

42 See, for example, the national positions of Brazil (2020), China (2021) (general), Kenya (2021).

43 See, for example, the national positions of China (2021) (general) and Russia (2021).

44 Comment made at the project roundtable on Latin America and Caribbean perspectives (report on file with authors).



c. Scenarios and examples

Several national positions refer to examples of malicious cyber operations to illustrate possible violations or highlight the importance of international law in the cyber context. Examples have ranged from general types of malicious cyber operations (such as cyber espionage, electoral interference, disinformation, and ransomware)⁴⁵ to real-world incidents (for example, the NotPetya cyberattack).⁴⁶ Two national positions go a step further and include more detailed hypothetical scenarios of cyber operations that could potentially violate international law.⁴⁷ The inclusion of examples or scenarios can enhance clarity and precision. In particular, they can elucidate the legal outcomes or implications of adopting a certain interpretation or advocating for a new rule of international law in the cyber context. They can also ensure that national positions are relevant and practical in the cyber context and do not constitute mere restatements of international law in the abstract. In particular, examples of real-world cyber incidents can set the scene and elucidate the motivation for issuing a national position. Examples or scenarios are also crucial if a State decides to follow the inductive approach in its position; that is, by starting from certain facts and then explaining how the law applies to them.

45 See, for example, the national positions of [Costa Rica \(2023\)](#), the [UK \(2022\)](#) and the [US \(2016\)](#).

46 See, for example, the national positions of the [UK \(2018 and 2022\)](#).

47 See, for example, the national positions of [Australia \(2021\)](#) and [Austria \(2024\)](#).



d. References

Most of the national positions published to date include references to relevant decisions of international courts and tribunals, treaties, UN documents (particularly the work of the International Law Commission), and academic sources (most notably the Tallinn Manuals). These references have taken the form of footnotes,⁴⁸ endnotes,⁴⁹ and/or bibliography.⁵⁰ **References can lend greater legal authority to a national position, making it more persuasive for different audiences, including other States and academics.** However, too many references can make a position visually clunky and cumbersome to read, especially if the references are footnoted. Therefore, effective referencing requires striking a balance between legal authority and accessibility. Hyperlinks to the materials cited in the footnotes can also improve accessibility by making it easier for readers to find the relevant documents. For more concise and informal national positions, such as those issued as UN statements or speeches later published as blogposts, an option is to include hyperlinks to referenced works in the body of the position rather than spelling out full citations in the footnotes.

e. Headings, summaries, and numbered paragraphs

The vast majority of published national positions employ headings. These can help structure a position around clear areas, topics, or questions of international law in the cyber context – usually from the most general to the most specific. **This can significantly improve a national position's clarity and readability.**

Summaries are also important for clarity and accessibility, especially for longer documents, as they can highlight the key messages conveyed in a national position. Summaries are particularly helpful for practitioners, including government lawyers and diplomats, who have limited time to read positions in full. Nevertheless, only six national positions published to date contain summaries (Australia (2017), Austria, Estonia (2021), France, Norway, and Poland). In the national positions of Austria, Estonia (2021), France, and Norway, the summaries are contained in text boxes, which further increases readability. In the national positions of Australia (2017) and Poland, the summaries appear in the form of headings with short sentences that capture the main takeaways of relevant sections. This helps the reader quickly identify what issues the position covers and what the main conclusions on these issues are.

48 See, for example, the national positions of [Austria \(2024\)](#), [Costa Rica \(2023\)](#), [Cuba \(2024\)](#), [Czechia \(2024\)](#), and [Ireland \(2023\)](#).

49 See, for example, the national positions of [Canada \(2022\)](#) and [Colombia \(2025\)](#).

50 See, for example, the national position of [Colombia \(2025\)](#).



Numbered paragraphs are also helpful for referencing specific points raised in the document, allowing others to easily cite the position. This should be considered if the aim of a position is to influence audiences, particularly other States and academics. However, only a few national positions and one common position published to date contain numbered paragraphs.⁵¹

f. Visual aids

Some national positions have been typeset into specially designed documents, such as the ones of Australia (2017 and 2021), Colombia, France (2019), and New Zealand. However, none features visual aids such as tables, charts, or infographics. These resources have been used successfully in other cyber policy documents, such as Australia's International Cyber Engagement Strategy (which, as noted, contains its 2017 national position as an annex),⁵² and explainers⁵³ on the 11 GGE norms of responsible State behaviour.⁵⁴ **Visual aids could be incorporated to increase the accessibility of national positions,** whether in the same document or in separate dissemination strategies, as discussed below.

51 National positions of Canada (2022), Costa Rica (2023), Cuba (2024), Czechia (2024), Ireland (2023), New Zealand (2020), Pakistan (2023), and the UK (2021), and also the common position of the AU (2024).

52 Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (October 2017), 8-9, 16, 85.

53 See, for example, Australian Strategic Policy Institute, International Cyber Policy Centre, *The UN norms of responsible state behaviour in cyberspace Guidance on implementation for Member States of ASEAN* (March 2022).

54 UN General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/70/174 (22 July 2015), para 13.



3. Language

For the purposes of this chapter, ‘language’ refers to the use of legal terminology and to the actual language(s) of publication.

a. Legal terminology

All national positions issued to date have employed traditional international law lexicon in their analysis of international rules, principles, and regimes as they apply in the cyber context. This is crucial if the aim of a position is to develop or clarify how international law applies in the cyber context. **But States should be precise and consistent when using legal terms**, such as ‘sovereignty’, ‘jurisdiction’, ‘attack’, and ‘coercion’. These and other words not only have a special meaning in international law but are also subject to significant debate. Therefore, it is important to clarify in a national position what a State means when using such terms. This includes not only providing a legal definition but also situating each concept within existing debates as well as indicating what view, if any at all, a State is advancing on the matter.

For example, when discussing sovereignty as it applies to cyber activities in its national position, it is helpful to specify whether a State is referring to the debate between sovereignty-as-a-principle and sovereignty-as-rule,⁵⁵ or to the corollaries of State sovereignty, such as jurisdiction and non-intervention.⁵⁶ Likewise, if the aim of a national position is to take a stance on those debates, it is important to clearly indicate what such a stance is. Conversely, if a State does not wish to take a firm position on a certain debate, whether because it has not made up its mind or the evidence is inconclusive, then it should say so in clear terms.

Key words have been used to communicate such intentions. For example, when a national position claims that a State ‘must’, ‘shall’, or ‘is required’ to do or refrain from doing something, it is expressing the view that the relevant behaviour is grounded in a binding legal obligation. Another way of expressing that a certain rule is binding under international law is to say that it constitutes *lex lata* (that is, what the law is). Conversely, the use of terms such as ‘should’, ‘may’, or ‘could’ implies that the State does not view the behaviour in question as required under international law.⁵⁷ Similarly, a State can say that a statement is *lex ferenda* (that is, what the law should be) or constitutes a ‘non-binding norm’ if it does not consider it to be binding under international law. Likewise, if a State considers that international law

55 See, for example, the national positions of [Austria \(2024\)](#), pp. 4-5, and the [UK \(2018\)](#), p. 7.

56 See, for example, the national position of [China \(2021\) \(sovereignty\)](#), p. 2.

57 See, for example, the national positions of [Canada \(2022\)](#), para 26, and [New Zealand \(2020\)](#), para 16.

is yet to regulate a certain behaviour, it can say that there is insufficient evidence of State practice and/or *opinio juris*,⁵⁸ that ‘further’ State practice and/or *opinio juris* is necessary,⁵⁹ or that it is ‘not convinced’ that the rule in question has ‘crystallized’.⁶⁰ On the other hand, if a State considers that the existing evidence of State practice and/or *opinio juris* is unclear or inconclusive for a definitive statement on the law, it may say that the relevant issue requires further study or ‘reflection’.⁶¹

The choice of words can also evince the legal status of a national position; that is, if the position is adopted as State practice and/or *opinio juris*, an interpretative aid, or a political statement.

It is also possible that the status of a national position varies depending on the issues or topics covered. For example, Estonia was likely expressing its *opinio juris* for the purpose of developing customary international law on collective countermeasures by saying that it was ‘furthering [a] position’ on the matter.⁶² In contrast, Norway made it clear at the outset of its national position that it was giving its ‘interpretation of certain obligations of international law as they apply to cyber operations’.⁶³ When a State uses hortatory language, such as by claiming that States ‘should’ behave in a certain way, it is likely making a mere political statement. Statements of this kind feature, for example, in the national positions of Canada, China, and New Zealand.⁶⁴

As noted in **Chapter 2**, national positions have also used **distinct terminology to promote different cyber legal policies**, including to confirm that existing international law is sufficient to regulate cyber activities or to argue that a new legally binding instrument is needed for them.⁶⁵ For example, Austria’s national position states that ‘international law applies in its entirety to cyber activities’ and that Austria ‘does not see a need for the development of a new legally binding instrument relating to international

58 See for example, the national positions of [Israel \(2021\)](#), p. 404, and the [UK \(2021\)](#), para 12.

59 See, for example, the national position of [Canada \(2022\)](#), para 25.

60 See, for example, national position [New Zealand \(2020\)](#), para 17.

61 See, for example, the national position of [Brazil \(2021\)](#), p. 23.

62 National position of [Estonia \(2019\)](#).

63 National position of [Norway \(2021\)](#), p. 2.

64 See the national positions of [Canada \(2022\)](#), para 26 ([‘n]o State should knowingly allow its territory to be used for acts contrary to the rights of other States); [China \(2021\) \(general\)](#), (for example, ‘iii. States should enhance critical ICT infrastructure protection’); and [New Zealand \(2020\)](#), para 16 (‘states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs’).

65 See, for example, the national positions of [China \(2021\) \(sovereignty\)](#), p. 1, [Cuba \(2024\)](#), paras 4-5, [Pakistan \(2023\)](#), para 8, and [Russia \(2021\)](#), p. 80.



cyber activities’.⁶⁶ Similarly, the common position of the EU argues that international law ‘fully applies to cyberspace’ and ‘is fit for purpose in this digital age’.⁶⁷ Conversely, the national position of China states that ‘[t]he international community should develop universally accepted norms, rules and principles within the framework of the UN, to jointly address the risks and challenges, and uphold peace, security and prosperity in cyberspace’.⁶⁸ In the same vein, the national position of Russia ‘advocates a broader idea of progressive development and improvement of international law taking into account the specific features of ICTs’ by ‘adopting a binding universal convention on international information security at the UN level’.⁶⁹

b. Language of publication and translation

The vast majority of the national positions and the two common positions issued to date have been published in English. English is the prevalent language in relevant legal, diplomatic, and academic settings, including in the GGE and OEWG as well as in the Tallinn and Oxford Processes. To ensure that positions are consistent with existing international law lexicon, clearly understood by a majority of stakeholders, and enhance common understandings among States, it is important to publish them in English. For example, in English, the term ‘norm’ has come to be understood as a non-binding expectation or standard of behaviour, such as the GGE’s norms of responsible State behaviour in cyberspace. However, the equivalent term in other languages, such as French (*norme*) or Italian, Portuguese, and Spanish (*norma*), can also refer to a binding rule. The same might be true of concepts in computer science and other technical fields, which have an established English terminology. **Therefore, using English in national positions can ensure clarity and precision as well as avoid misunderstandings, especially when it comes to legal and other technical terms.**

A few States have opted to publish their national position in other languages. This has been the case of States whose official language is not English. Examples include the national positions of France (published in French in 2019 and translated into English in 2021),⁷⁰ Finland (published in Finnish and English in 2020),⁷¹ Kazakhstan (published only in Russian in the GGE Official Compendium in 2021), Switzerland (published in English and French in the GGE Official Compendium in 2021), Russia (published in English and Russian

66 National position of [Austria](#) (2024), p. 3. See also, for example, the national position of [Costa Rica](#) (2023), para 7.

67 Common position of the [EU](#) (2024), pp. 3-4.

68 National position of [China](#) (2021) (general), p. 1.

69 National position of [Russia](#) (2021), p. 80.

70 National position of [France](#) (2021).

71 See the [Finnish](#) and [English](#) versions of the national position of Finland (2020).

in the GGE Official Compendium in 2021), Cuba (published in Spanish in 2024), and Colombia (published in English and Spanish in 2025). Canada published its national position in 2022 in its two official languages: English and French.⁷² The UK's 2021 national position was published in the GGE Official Compendium in all official languages of the UN: Arabic, Chinese, English, French, Russian, and Spanish.

Publishing a national position in languages other than English can serve a variety of purposes.

First, it can increase the accessibility of a position to non-English speaking audiences domestically and/or internationally. While English is the most spoken language in the world, the vast majority of the population living in the Global South does not speak English: at the time of writing, about 13% of the world's population speak English and only 5% are native English speakers.⁷³ Mandarin Chinese, Hindi, Spanish, French, and Arabic follow English as the most spoken languages.⁷⁴ Therefore, a multilingual publication strategy focussing on one or more of these languages can enhance inclusivity, bridge knowledge gaps, and reduce digital divides. Second, as underscored by several State representatives during the project roundtables, publishing a national position in one or more other languages than English can ensure that domestic stakeholders, including in government and civil society, not only understand a national position but also feel ownership over the process and its outcome.⁷⁵ Likewise, if a national position is developed domestically or regionally in a language other than English, then publishing the position in that language can ensure consistency in legal terminology and meaning. Relatedly, each language, region, and/or country has its own legal and cultural traditions and expressions. Therefore, publishing a national position in a local language can capture those traditions and expressions, ensuring that the position is relevant and sensitive to the local context. Finally, issuing a national position in multiple languages, as the UK did in 2021, can ensure control over official translations and therefore consistency in meaning across them.

72 National position of Canada (2022) ([English](#) and [French](#) versions).

73 Encyclopaedia Britannica, 'Languages by total number of speakers'; Dylan Lyons, 'How Many People Speak English, And Where Is It Spoken?', *Babbel* (10 March 2021); Encore, 'What Is the Most Spoken Language in the World'.

74 See Encyclopaedia Britannica, 'Languages by total number of speakers'; Wikipedia, 'List of languages by total number of speakers'; Statista, 'The most spoken languages worldwide in 2023'.

75 Comments made at the project roundtables on Asia and Pacific perspectives and on Latin America and Caribbean perspectives (reports on file with authors).



However, some considerations should be borne in mind when deciding whether a position is to be published in or translated into languages other than English. As noted above, some legal and other technical terms might have a different meaning or simply do not exist in other languages. For example, the concept of ‘sovereignty-as-a-rule’ does not translate easily into French, giving rise to ambiguity.⁷⁶ This means that at least a version of a national position should be published in English if its aim is to develop or clarify international law as it applies in the cyber context. Furthermore, whether a national position is originally published in English or another language, **it is important to ensure that any translation is accurate and consistent.**



⁷⁶ See Aude G ry, ‘Navigating France’s Views on Sovereignty in Cyberspace: Why Might France Not Be in the “Sovereignty-As-A-Rule” and in the “Pure Sovereignty” Camps,’ *EJIL: Talk!* (19 September 2024).

4. Dissemination

National positions are official documents of a legal and/or political nature. As such, they have been published and disseminated through **formal government and diplomatic channels**. As noted in **Chapter 3**, these include official gazettes and press releases,⁷⁷ government websites,⁷⁸ and domestic or international online repositories, such as the UN Digital Library (for the national positions found in the GGE Official Compendium)⁷⁹ and the OEWG's document database⁸⁰ (where many standalone national positions have been published). Making national positions available through such channels enhances their authority and ensures that legal and diplomatic audiences who are familiar with those channels can easily find them. **It is particularly helpful to publish national positions on the OEWG's document database** since it is a well-known platform for official documents relevant to its discussions on the implications of ICTs for peace and security. This can ensure that not only governments but also other stakeholders who follow the OEWG process (such as industry, civil society, and academia) have access to national positions.

As noted above, some national positions have been published as **academic articles**. In the case of Denmark, the national position was exclusively published as an academic article. In other cases, the article is a transcript of an official speech (for example, Israel and the US (2016)) or a republication of a standalone position paper (for example, Finland, Norway, and Sweden). This dissemination strategy might be appropriate to target academic audiences. However, as noted, academic articles might not be readily accessible to other audiences, either because of their format and style or because of their reach, since non-specialists might not be familiar with academic publications.

Publishing a national position, or a version thereof, on a **blog** can also increase its reach among non-expert audiences. For example, the position of Israel was originally delivered as a speech that was also published on the *EJIL: Talk!* blog.⁸¹ This increased the visibility of the position among international lawyers and non-specialists who follow that blog.

77 See, for example, Council of the EU, 'Cyberspace: Council approves declaration on a common understanding of application of international law to cyberspace' (18 November 2024).

78 See, for example, the national positions of [Canada \(2022\)](#), [France \(2019\)](#), [the Netherlands \(2019\)](#), and the UK (2018, 2021 and 2022).

79 UN Digital Library.

80 UNODA, Open-Ended Working Group on Information and Communication Technologies, [Documents](#).

81 Roy Schöndorf, 'Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations,' *EJIL: Talk!* (9 December 2020).



A commentary on the common position of the AU, authored by its principal drafter (Mohamed Helal, the AU special rapporteur on international law in cyberspace) was published on the same blog.⁸² The post included remarks on the topics covered by the common position as well as the process that led to its adoption by the AU. This not only increased the visibility of the common position but also the interest in it. Blogposts can be particularly helpful in explaining a national position to non-specialists, especially if written in more accessible language without legal or technical jargon.

Whether published as a speech, UN statement, standalone written document, or academic article, **the vast majority of national positions issued to date can be found online.** As noted above, this includes government websites, the online versions of academic journals, and the OEWG's document database.⁸³ Unofficial databases have also republished national positions online. The *Cyber Law Toolkit*⁸⁴ is one of the most popular ones, with national positions arranged by country and topic in an accessible format. The UN Institute for Disarmament Research's *Cyber Policy Portal* also showcases national positions by country, using an interactive world map.⁸⁵

Publishing national positions online is important for several reasons.

First, target audiences – whether in government, industry, or civil society – are spread around the world and many are unable to attend the meetings or events where national positions are announced, read out or discussed. Second, online consumption habits are increasing among all demographics. Third, publishing national positions online is more efficient, including in terms of time and cost, as well as more environmentally friendly. Fourth, digital formats facilitate keyword searches and automated translations, making it easier for audiences to access national positions in different languages. In sum, publishing a national position online ensures that it can be easily and quickly accessed by all relevant stakeholders, regardless of their physical location.

82 Mohamed Helal, 'The Common African Position on the Application of International Law in Cyberspace: Reflections on a Collaborative Lawmaking Process,' *EJIL: Talk!* (5 February 2024).

83 UNODA, Open-Ended Working Group on Information and Communication Technologies, Documents.

84 See the <https://cyberlaw.ccdcoe.org>

85 See UNIDIR, *Cyber Policy Portal*.



Relatedly, using **social media channels** to announce the publication of a national position and/or comment on it can be an efficient dissemination strategy among expert and non-expert audiences.⁸⁶ Many diplomats, government lawyers, industry representatives, and academics have a social media profile and follow developments in cyber policy or international law in cyberspace through their social media networks. Likewise, many members of the public are avid users of social media. Therefore, it is more likely that they will see and engage with the publication of a national position if it is announced in a post on social media. Social media posts can also be used to raise awareness of a national position published in English to non-English speaking audiences and vice-versa, especially if there is no capacity to arrange an official translation of the position itself to other languages. Video explainers published on social media and other online platforms can also help raise awareness of national positions and increase their accessibility to different audiences, particularly among non-experts.

Another dissemination strategy to increase the visibility and impact of a national position is to organize **public and/or private events** to publicize the document and/or to discuss its contents with different stakeholders. As noted above, this could be done when a national position is delivered as a speech at conferences or special events, as in the case of the national positions of Estonia (2019), Israel, the UK (2018 and 2022), and the US (2012, 2016, and 2020). Furthermore, side-events in the margins of the OEWG and its future permanent mechanism in New York can be a good opportunity to announce and to publicize a national position. For example, in March 2024, an OEWG side-event was held to disseminate the common position of the AU among UN and African audiences, which could participate in the event online. National or regional dialogues and academic conferences can also be organized to sensitize local audiences about the publication of a national position. For example, Italy's national position was discussed at a conference at the University of Bologna in November 2021.⁸⁷ Such events are particularly helpful if they provide local audiences with an opportunity to discuss, in local languages, a national position that was only published in English.

86 For example, Bert Theuermann, *X Post* (31 May 2024); Republic of Poland ('Rzecznik MSZ'), *X Post* (29 December 2022); Foreign Policy Canada, *X Post* (28 April 2022); Germany in the United Nations, *X Post* (9 March 2021).

87 See François Delerue, 'Conference on "The Application of International Law to Cyberspace" organised at the University of Bologna,' *EU Cyber Direct* (12 November 2021).



Finally, States should consider including **visual aids** as part of an overarching communications strategy. Several State representatives consulted in the context of this project emphasized that work on the substance of a national position should be accompanied by proper attention to presentation. As noted above, visual aids can include typesetting, infographics, tables, and charts.



Figure 11: Examples of dissemination strategies for national positions.

5. Conclusion

As discussed throughout this chapter, there are pros and cons to each choice of format, style, language, and dissemination for a national position. Ultimately, these choices should be informed by the legal status, approach, and aims States set for their positions. For example, if a national position is published as evidence of a State's *opinio juris* or its interpretative views and seeks to influence the development or interpretation of international law, a well-structured and detailed written document, published in English, might be more appropriate. Conversely, if a national position aims to make policy comments on or raise awareness of general issues of international law in cyberspace, then a shorter, less-structured document or speech, published in English and/or other language(s), might suffice. Nevertheless, whatever the status, approach, and aims of a national position, its content needs to be clearly understood and given appropriate weight by relevant audiences. Therefore, States should strike a delicate balance between authority and accessibility when considering how to present their national positions.

Following the tried-and-tested trends in format, style, language, and dissemination strategies discussed in this chapter can be an effective way to strike this balance. It can also help States and other stakeholders compile, compare, and contrast national positions with a view to finding areas of consensus, disagreement, and gaps in the understanding of how international law applies in the cyber context. However, each State has distinct needs, aspirations, and cultural and legal traditions. Therefore, as with the choice of substantive issues to cover and of the process to follow, there is no single presentation template for national positions. Instead, there is a menu of options and elements that can be mixed and matched to fit different intentions. It is for States to decide which of these options to follow, or whether to set new trends.



CHAPTER 6:

CONCLUSION

6



National positions have changed the way international law is understood in the cyber context. As an increasing number of States have published their views on how international law applies to cyber activities, the field has moved further away from grey zones and closer to greater clarity. To be sure, uncertainty and disagreements remain about *which* international rules and principles apply to information and communications technologies (ICTs), *how* they apply, and *whether* developing new rules is necessary. Full alignment on these issues is virtually impossible and may not even be desirable: international law is vast, many of its questions are complex, and a multitude of States and other actors with different histories, cultures, and agendas are involved in developing, interpreting, and applying the law. However, as discussed throughout this Handbook, national and common positions have made it much easier to map out areas of convergence and divergence, as well as possible gaps. This mapping is crucial to foster dialogue and to build confidence among States, driving progress in the field, even when common understandings may not be possible.

In this sense, national positions have become an invaluable tool for States and other stakeholders in the field, including academics, industry representatives, and members of civil society. At the time of writing, 33 States have published a national position and two regional organizations – the African Union (AU) and the European Union (EU) – have published common positions (see **Annex B**). A number of other States have expressed interest in developing a national position, while some of those with existing positions may wish to review or update them. To guide them through the process of developing or reviewing a national position, this Handbook has explored key questions that might arise along the way.

First, as noted in the **Introduction**, national positions may have legal implications in the cyber context and beyond. Specifically, they may qualify as evidence of *opinio juris* and, more controversially, as State practice. As such, they can contribute to the development of customary international law. Likewise, national positions may constitute subsequent practice in the application of international treaties or supplementary means to interpret those treaties. There is also debate as to whether the silence of States that are yet to publish a national position can constitute acquiescence to the customary rules or treaty interpretations advanced by other States in their positions. Under international law, the silence of States can only amount to acquiescence to a customary rule or treaty interpretation if certain stringent conditions are met.



These include the existence of sufficiently specific circumstance calling for a reaction, proper knowledge, and the passage of a reasonable amount of time.¹

In many respects, the legal impact of national positions has not been limited to cyber activities and has extended to international law as a whole. The trend of publishing national positions was prompted by the difficulty of applying old law to a new and pervasive technology: malicious cyber operations have been carried out at an unprecedented speed and had widespread impacts across national borders, challenging traditional concepts of international law, such as sovereignty, non-intervention, and the notions of 'attack' and 'object' in international humanitarian law (IHL). By exploring how international rules and principles of general applicability ought to be understood in the cyber context, national positions have revived foundational debates that are relevant in other contexts. Examples include whether sovereignty and due diligence give rise to State obligations and whether third States can resort to collective countermeasures.

Chapter 2 unpacked the various motivations for developing a national position (or choosing not to do so). Three overarching functions have been identified: to communicate to different stakeholders the views of a State on the application of international law to cyber activities (communicative function); to transform or to adapt the rules of international law as they apply in this context, including by developing customary international law or by proposing new treaty interpretations (transformative function); and to deter, to prevent, and/or to mitigate the negative consequences of malicious cyber operations carried out by States and non-State actors (preventative function).

These functions might be fulfilled through specific aims and articulated as different motivations. In particular, national positions can prevent miscalculation and escalation by increasing predictability and stability in international relations. Likewise, they can enhance compliance and accountability by deterring and preventing unlawful cyber operations. National positions can also shape the evolution of international law as it applies to cyber activities and address legal uncertainty. Additionally, the positive impact of national positions can be felt domestically. In particular, they can help clarify what responsible State behaviour means for domestic stakeholders, foster national cyber resilience, improve interagency coordination, and drive important legal and policy developments.

¹ ILC, *Draft conclusions on the identification of customary international law, with commentaries*, A/73/10 (2018), 120, conclusion 10(3); ILC, *Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties*, (2018), 15, conclusion 10(2).



However, several factors might make it difficult for States to achieve those aims. Central among these is lack of capacity. The vast majority of the national positions published to date have been issued by developed countries. And the development of the common position of the AU was made possible thanks to concerted capacity-building efforts and strong leadership by the organization.² The development of a national position is a resource-intensive process, and significant investments are needed to close the capacity gap between developed and developing countries. At the same time, some States may lack the necessary political will to embark on the process of developing a national position. Other States might fear that they will constrain their freedom of action or prompt yet more disagreements about how international law applies to cyber activities by issuing a national position. Therefore, it is important to continue to discuss the various functions and aims of national positions, underscoring that they can foster transparency and build confidence among States even when common understandings on substance cannot be reached.

Chapter 3 unpacked the various steps that might be involved in the development of a national position. As a starting point, States should consider identifying which internal and external stakeholders they want to involve in the process, bearing in mind that a combination of legal, policy, and technical expertise is highly recommended. It may also be useful to designate a particular agency as the penholder tasked with the coordination of the process and the drafting of the position. A series of organizational steps might need to follow. These include assigning roles to different stakeholders and considering questions such as the scope and aims of the position, the location of relevant meetings and other tasks, the timeframe, and the various methods for carrying out each task. Some States may also welcome capacity-building on different topics, including international law, cyber policy, and cyber security, before they can develop a national position.

When it comes to the drafting of a national position, States can follow different strategies. For example, they may start from a comprehensive text and narrow it down following discussions. Conversely, a simpler text or outline may be developed into a fully-fledged position paper.

2 Mohamed Helal, 'The Common African Position on the Application of International Law in Cyberspace: Reflections on a Collaborative Lawmaking Process,' *EJIL: Talk!* (5 February 2024).



During the drafting stage, States may resort to formal and informal sources as well as consultations with internal or external stakeholders. The adoption of a national position may also need to follow a defined institutional process, including a formal sign-off by a specific authority. National positions may be subject to review, as States can decide to adjust or to revise their original stance on the various issues at stake.

These various steps and drafting strategies reveal that the task of developing and publishing a national position is far from trivial, and that it might be especially difficult for States facing capacity gaps or political hurdles. Frustratingly, the hard work put into this process by all the stakeholders involved might not culminate in a published position. But this should not discourage States. The process itself is valuable, irrespective of its outcome. It can, for example, foster greater dialogue and coordination between domestic agencies, help States formulate internal positions that need not be published, and better prepare them for discussions in multilateral processes. In particular, the knowledge gained during the training, discussion, and/or drafting sessions for a national position can be used in diplomatic negotiations and more targeted submissions in the UN Open-Ended Working Group (OEWG) and other multilaterals forums. As noted in different chapters of this Handbook, States can also use those submissions to express their views on how different rules and principles of international law apply to cyber activities.

Chapter 4 provided an overview of the various substantive issues covered in national positions to date, as well as the policy considerations underlying how States have selected and approached those issues. While there is some variation in their choice of topics as well as their depth of analysis, the national positions published to date feature a broadly consistent list of issues or areas of international law. These include foundational rules and principles, such as the principle of sovereignty and its corollaries, including non-intervention, the prohibition of the use of force, and due diligence, as well as peaceful settlement of disputes and self-determination. National positions also address specialized regimes of international law, including, in particular, IHL, international human rights law (IHRL), and international criminal law. State responsibility, which governs the consequences of breaches of international obligations, is also a popular topic, including attribution, countermeasures, and necessity.



National positions can help States understand their differences, constructively debate them, and strive for common ground when there is opportunity to do so.

National positions have fostered agreement on some of those issues, including, as a starting point, that international law applies to cyber activities. There is also agreement that IHL and IHRL are in principle applicable

to ICTs. Moreover, a consensus is emerging around the components of specific rules or principles, such as non-intervention and State responsibility. However, as noted, national positions have revealed areas of disagreement. These include whether certain principles also give rise to obligations, the thresholds or conditions triggering a violation of certain obligations, and whether and to what extent certain types of cyber activity – such as cyber espionage – may constitute violations. As noted, some disagreement is inevitable, especially in a decentralized legal system like international law. Likewise, not all disagreements are necessarily detrimental to international peace and security. But, crucially, disagreements need to be known in order to be discussed and, if necessary, addressed. National positions can help States understand their differences, constructively debate them, and strive for common ground when there is opportunity to do so.

It is not only the substance of national positions that matters: their presentation is just as important as it will dictate the impact that they might have. **Chapter 5** discussed the various options that States have for the format, style, language, and dissemination of their national position. These features vary significantly among the national positions published so far and they reflect important policy choices, including on the legal status, approach, and aims of such positions. While some national positions were issued as government speeches, UN statements, and academic articles, the vast majority have been published as standalone written documents. Their style has also oscillated between short documents of two to five pages and longer documents of up to 22 pages. The shorter national positions are naturally more general, sometimes prioritizing questions of policy. Longer positions cover more ground and delve deeper into specific legal questions, which makes them more suitable if the aim is to clarify and/or develop international law as it applies to cyber activities. Most national positions contain references and headings, which can increase their legal authority, readability, and clarity. Summaries, numbered paragraphs, examples, and visual aids can also significantly increase the accessibility of a position, but only a few incorporate those elements.



All national positions employ traditional international law lexicon and use specific terminology to indicate their stance on different legal issues. Most national positions and the two common positions have been published in English, the lingua franca of international law and diplomacy. This has ensured the use of consistent legal terminology and visibility among relevant audiences, including government lawyers, diplomats, and academics. However, to increase the accessibility of national positions to other audiences, especially domestic and foreign stakeholders in the Global South, States may want to consider publishing their national positions in languages other than English, including the other official languages of the UN (Arabic, Chinese, French, Russian, and Spanish). States should also consider different strategies to disseminate their positions to target audiences, including publishing them on relevant online databases, academic journals, blogs, and social media as well as organizing public and private events to discuss them. Overall, when deciding which format, style, language, and dissemination strategies to go for, States should seek to strike a balance between legal authority and accessibility.

What comes next?

If national positions have become the primary vehicle through which States express their views on international law in the cyber context, more States should feel empowered to develop and publish their positions *if they so wish*. As discussed earlier, this requires concerted efforts to raise awareness about the importance of national positions as well as to develop the capacity of States on the substance of international law and the process of developing positions, prioritizing those most in need.

As noted in the Introduction, the core team behind this project engaged in three regional consultations with representatives of States from Africa, the Americas, and Asia and the Pacific. The aim was to exchange views on the various topics addressed in this Handbook and to understand what is needed to bridge capacity gaps between States. Nevertheless, there is scope to extend those discussions to other regions, in particular Eastern Europe and the Middle East, with due consideration of linguistic and cultural differences that might affect the understanding of international law in those regions. The topic could also benefit from more in-depth discussions in international forums, including the UN. The future permanent mechanism that might succeed the OEWG in overarching discussions about the security implications of ICTs would be particularly well placed to continue the conversation about national positions within the UN.³

3 See UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, A/79/214*(2024), paras 5, 7, 56-60.



There has also been some discussion about the adoption of other instruments or materials on the application of international law to the cyber context. For example, the common position of the AU suggests that ‘the process of articulating rules of international law that apply to the use of ICTs in cyberspace would benefit from the adoption of a United Nations declaration on this subject’.⁴ It is unlikely that the UN Security Council would adopt a resolution on the application of international law to cyber activities, given persistent disagreements between its permanent members. On the other hand, a majority of UN member States could support the adoption of a resolution on the topic by the UN General Assembly, perhaps grounded in the work of the OEWG’s successor. Nevertheless, the content of this declaration would probably be general, like most UN General Assembly resolutions adopted so far.

Some have also called for the General Assembly or another competent UN body to request an Advisory Opinion from the International Court of Justice (ICJ) on the application of international law to cyber activities.⁵ However, the ICJ might not be well placed to resolve this question, given that a significant number of areas and issues of international law, from general rules and specialized regimes to questions of State responsibility, are relevant to cyber activities. Others have speculated that the International Law Commission would initiate a study and eventually issue a report on the topic, but there has been no sign of such a move at the time of writing. However, it should be noted that the issue of applying international law to cyber activities is currently under consideration by the Institut de Droit International.⁶

4 Common position of the AU (2024), para 7.

5 See Statute of the International Court of Justice, Article 96.

6 Institut de Droit International, *The Applicability of International Law to Cyber Activities* (2023).



As discussed in this Handbook, some States have called for a legally binding treaty to govern different aspects of ICTs, such as information or data security.⁷ Different stakeholders have also proposed the adoption of a treaty to expand the protections already offered by existing international law in the cyber context, such as a digital Geneva Convention or a convention for the protection of critical infrastructure from cyber operations.⁸ While these proposals may or may not materialize, they are not necessarily at odds with efforts to clarify how existing international law applies to cyber activities, including through national positions. Both types of initiatives can coexist and complement one another.

National positions can also catalyse the adoption of domestic legislation and policy documents to internalize and further develop standards of responsible State behaviour in the cyber context. In particular, States can articulate through national laws what practical steps they believe should be taken domestically to implement obligations such as sovereignty, non-intervention, and due diligence as well as human rights protections against cyber operations. Similarly, States can incorporate and develop their views on how IHL applies to ICTs in their own military manuals or rules of engagement.

Whether domestically or internationally, there is also scope for more practical discussions about the content of national positions, such as through scenario-based exercises or case studies. As noted in **Chapter 5**, many national positions delve deep into the complexities and controversies of different international rules and principles that are particularly relevant in the cyber context. However, they do so, for the most part, in a very abstract way, with only a few positions referencing real-life incidents, including examples of cyber operations that could hypothetically breach international law, or proposing practical steps to implement international obligations in the cyber context.

Last, given the overall positive impact of national positions, including on international law in general, the model can be leveraged to foster dialogue and common understandings on other global challenges that have given rise to legal uncertainty and disagreements among States. This is particularly the case with issues for which there is no specific treaty and/or permanent forum for multilateral discussions or adjudication; for example,

7 For example, Russian Federation, *Updated Concept of the Convention of the United Nations on Ensuring International Information Security*, (2023); People's Republic of China, *Global Initiative on Data Security*, (2022).

8 See, for example, Patryk Pawlak and Aude Géry, 'Why the World Needs a New Cyber Treaty for Critical Infrastructure', Carnegie Endowment for International Peace (28 March 2024); Microsoft, 'The need for a Digital Geneva Convention' (14 February 2017).



other emerging technologies like artificial intelligence. In fact, States have already started to publish national views on how they think international law, especially IHL, applies to lethal autonomous weapons systems.⁹ And the UN General Assembly has recently invited member States to submit their views on the international peace and security implications of the use of artificial intelligence in the military domain, beyond lethal autonomous weapons, including how international law addresses the issue.¹⁰

Other areas such as outer space and human rights in armed conflict might equally benefit from statements on how existing international law addresses emerging challenges, giving their rapidly changing landscape and the absence of a dedicated multilateral forum. These statements need not be as comprehensive as the national positions published in the context of ICTs, since many of the latter already cover general international law questions in great detail (for example, sovereignty, non-intervention, and due diligence). National positions on artificial intelligence and other issues could build on this acquis, targeting more specific questions of international law that pose concrete challenges in those contexts.

Whatever the future holds for national positions, and irrespective of whether new instruments or further agreement on international law in the cyber and other contexts come about, one thing is clear: the positions published so far are a testament to the progress that States have already made, and can continue to build on, in a challenging environment. They are a sign that, even if legal differences and geopolitical tensions remain, constructive dialogue is possible. We hope this Handbook can inspire States to continue on this path, thus fostering transparency, discussion, and shared understandings on how international law can help address the world's greatest challenges – online and offline.

⁹ See UN General Assembly, *Lethal autonomous weapons systems: Report of the Secretary-General*, A/79/88 (1 July 2024).

¹⁰ UN General Assembly, *Artificial intelligence in the military domain and its implications for international peace and security*, A/RES/79/239 (31 December 2024).





BIBLIOGRAPHY

Books and monographs

Cryer, Robert, Robinson, Darryl, and Vasiliev, Sergey, An Introduction to International Criminal Law and Procedure (CUP 2019).

Dias, Talita, Beyond Imperfect Justice: The Principles of Legality and Fair Labelling in International Criminal Law (Brill 2022).

Gallant, Kenneth S, The Principle of Legality in International and Comparative Criminal Law (CUP 2010).

Knop, Karen, Diversity and Self-Determination in International Law (CUP 2009).

Lahmann, Henning, Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution (CUP 2020).

Milanovic, Marko, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy (OUP 2011).

Roscini, Marco, Cyber Operations and the Use of Force in International Law (OUP 2014).
– International Law and the Principle of Non-Intervention (OUP 2024).

Schabas, William A, The Customary International Law of Human Rights (OUP 2021).

Sparks, Tom, Self-Determination in the International Legal System (Bloomsbury 2023).

Sterio, Milena, The Right to Self-Determination under International Law (Routledge 2013).

Urs, Priya, Dias, Talita, Coco, Antonio, and Akande, Dapo, The International Law Protections against Cyber Operations Targeting the Healthcare Sector (ELAC 2023).

Zoller, Elizabeth, Peacetime Unilateral Remedies: An Analysis of Countermeasures (Transnational 1984).

Edited books and reference texts

Fisher, Ryan (ed), Operational Law Handbook (National Security Law Department, the Judge Advocate General's School, United States Army, 2022).

Henckaerts, Jean-Marie, and Doswald-Beck, Louise (eds), Customary International Humanitarian Law: Volume I, Rules (ICRC and CUP 2005).

ICRC (ed), Commentary on the Third Geneva Convention (CUP 2021).

Schmitt, Michael N (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017).

Contributions to edited collections

Akande, Dapo, 'Sources of International Criminal Law', in Antonio Cassese (ed), The Oxford Companion to International Criminal Justice (OUP 2009).



Hollis, Duncan B, and van Benthem, Tsvetelina, 'Threatening Force in Cyberspace', in Laura A Dickinson, and Edward W Berg (eds), *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold* (OUP 2024).

Mačák, Kubo, and Gisela, Laurent, 'The Legal Constraints of Cyber Operations in Armed Conflicts', in Rajeswari Pillai Rajagopalan (ed), *Future Warfare and Technology: Issues and Strategies* (Wiley 2022).

Pellet, Alain, 'Peaceful Settlement of International Disputes' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (online edn, OUP 2013).

Tams, Christian, 'Article 2(4)' in Bruno Simma et al (eds), *The Charter of the United Nations: A Commentary*, Vol I (OUP 2024).

Tomuschat, Christian, 'Article 2(3)' in Bruno Simma et al (eds), *The Charter of the United Nations: A Commentary*, Vol I (OUP 2024).

Tsagourias, Nicholas, 'Cyber Disputes as International Legal Disputes', in Nicholas Tsagourias, Russell Buchan, and Daniel Franchini (eds), *Peaceful Settlement of Interstate Cyber Disputes* (Hart 2024).

– 'Electoral Cyber Interference, Self-Determination and the Principle of Non-intervention in Cyberspace', in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy* (Rowman & Littlefield 2020).

Ziegler, Katja S, 'Domaine réservé' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (online edn, OUP 2013).

Journal articles

Cleveland, Sarah H, 'Embedded International Law and the Constitution Abroad' (2010) 110 *Columbia Law Review* 225.

Coco, Antonio, and de Souza Dias, Talita, "'Cyber Due Diligence": A Patchwork of Protective Obligations in International Law' (2021) 32 *European Journal of International Law* 795.

Coco, Antonio, Dias, Talita, and van Benthem, Tsvetelina, 'Illegal: The SolarWinds Hack under International Law' (2022) 33(4) *European Journal of International Law* 1275.

Deeks, Ashley, 'Defend Forward and Cyber Countermeasures', Hoover Working Group on National Security, Technology, and Law (2020).

Dias, Talita, 'Finding Common Ground: The Right to be Free from Incitement to Discrimination, Hostility, and Violence in the Digital Age' (2024) 16(4) *Global Responsibility to Protect* 391.

Droege, Cordula, 'Elective affinities? Human rights and humanitarian law' (2008) 90 *International Review of the Red Cross* 501.

– 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94(886) *International Review of the Red Cross* 533.

Egan, Brian J, 'International Law and Stability in Cyberspace' (2017) 35(1) *Berkeley Journal of International Law* 169.

Engdahl, Ola, 'Sweden's Position Paper on the Application of International Law in Cyberspace' (2023) 92(3) *Nordic Journal of International Law* 489.



Helal, Mohamed, 'On Coercion in International Law' (2019) 52(1) *NYU Journal of International Law and Politics* 1.

Henriksen, Anders, 'The end of the road for the UN GGE process: The future regulation of cyberspace' (2019) 5(1) *Journal of Cybersecurity* 1.

Jackson, Miles, and Paddeu, Federica, 'The Countermeasures of Others' (2024) 118(2) *American Journal of International Law* 231.

Kjelgaard, Jeppe Mejer, and Melgaard, Ulf, 'Denmark's Position Paper on the Application of International Law in Cyberspace' (2023) 92(3) *Nordic Journal of International Law* 446.

Lahmann, Henning, 'The Plea of Necessity in Cyber Emergencies' (2023) 92(3) *Nordic Journal of International Law* 422.

Lehto, Marja, 'Finland's views on International Law and Cyberspace' (2023) 92(3) *Nordic Journal of International Law* 456.

Mačák, Kubo, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 *Israel Law Review* 55.

Mendelson, Maurice, 'The Formation of Customary International Law' (1998) 272 *Recueil des Cours* 155.

Milanovic, Marko, and Schmitt, Michael N, 'Cyber attacks and cyber (mis)information operations during a pandemic' (2020) 11(1) *Journal of National Security Law and Policy* 247.

Musæus, Vibeke, 'Norway's Position Paper on International Law and Cyberspace' (2023) 92(3) *Nordic Journal of International Law* 470.

Ohlin, Jens D, 'Did Russian Cyber-Interference in the 2016 Election Violate International Law?' (2017) 95 *Texas Law Review* 1579.

Petridou, Evangelia, 'Theories of the Policy Process' (2014) 42 *Policy Studies Journal* S12.

Roscini, Marco, 'Gravity in the Statute of the International Criminal Court and Cyber Conduct that Constitutes, Instigates or Facilitates International Crimes' (2019) 30 *Criminal Law Forum* 247.

Schmitt, Michael N, and Watts, Sean, 'Collective cyber countermeasures?' (2021) 12 *Harvard National Security Journal* 373.

Schöndorf, Roy, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97 *International Law Studies* 395.

Shany, Yuval, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law' (2013) 7 *The Law and Ethics of Human Rights* 47.

Shany, Yuval, and Schmitt, Michael N, 'An International Attribution Mechanism for Hostile Cyber Operations' (2020) 96 *International Law Studies* 196.

van Benthem, Tsvetelina, Dias, Talita, and Hollis, Duncan B, 'Information Operations under International Law' (2022) 55 *Vanderbilt Journal of Transnational Law* 1217.



Selected reports and other online sources

Australia, Australia's Cyber Security Strategy (2016).

– Department of Foreign Affairs and Trade, Australia's International Cyber Engagement Strategy (October 2017).

Australian Strategic Policy Institute, International Cyber Policy Centre, The UN norms of responsible state behaviour in cyberspace Guidance on implementation for Member States of ASEAN (March 2022).

Austria, Pre-Draft Report of the OEWG – ICT: Comments by Austria (31 March 2020).

Chatham House, Applying the Plea of Necessity to Cyber Operations, Meeting Summary, International Law Programme (27 September 2023).

Chile, Ministry of Exterior Relations, Derecho Internacional, UN, New York, OEWG, Sixth Substantive Session (11-15 December 2023).

– National Cybersecurity Policy (2017-2022).

China (People's Republic of), Global Initiative on Data Security (2022).

Chinese Mission to the UN, Statement by the Chinese Delegation at the Thematic Debate of the First Committee of the 72th UNGA (2017).

Christou, George, 'Cyber Diplomacy: From Concept to Practice', Tallinn Paper No 14, NATO CCDCOE (2024).

Council of the European Union, 'EU sanctions – New recital in Council Decision', (CFSP) 2023/191 of 27 January 2023 – Countermeasures, WK 5169/2023 INIT (2023).

Cuba's Representative Office Abroad, 71 UNGA: Cuba at the final session of the Group of Governmental Experts on the developments in the field of information and telecommunications in the context of international security (23 June 2017).

Dias, Talita, Countermeasures in international law and their role in cyberspace (Chatham House 2024).

Estonia, Ministry of Foreign Affairs, Tallinn Workshops on International Law and Cyber Operations, Compendium of reports (2023).

European Commission, The EU's Cybersecurity Strategy for the Digital Decade (2020).

Germany, Federal Foreign Office, "'Cyber Security as a Dimension of Security Policy". Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London' (18 May 2015).

ICRC, International humanitarian law and the challenges of contemporary armed conflicts (October 2015).

– International humanitarian law and cyber operations during armed conflicts (2019).

– How is the term "armed conflict" defined in international humanitarian law?, Opinion Paper (2024).

Kavanagh, Camino, The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century, UNIDIR (2017).

McLaughlin, Robert, 'Data as a Military Objective', Australian Institute of International Affairs (20 September 2018)



Microsoft, 'The need for a Digital Geneva Convention' (14 February 2017).

Moynihan, Harriet, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* (Chatham House 2019).

National Cybersecurity Guide, *Guide to Developing a National Cybersecurity Strategy*, 2nd edition (2021).

Pacific Islands Forum, *Statement delivered by PIF Chair on behalf of the Pacific Islands Forum*, UN (New York, 4 December 2024).

Permanent Mission of Lichtenstein to the United Nations, *The Council of Advisers' Report on the Application of the Rome Statute to Cyberwarfare* (August 2021).

Persi Paoli, Giacomo, Dominion, Samuele, Rafiq, Aamna, and Filipová, Lenka, *Accelerating ICT Security Capacity-Building: Takeaways from the Global Roundtable on ICT Security Capacity-Building*, UNIDIR, Geneva (2024).

Russian Federation, *Updated Concept of the Convention of the United Nations on Ensuring International Information Security* (2023).

South Africa, *Statement by South Africa in the ninth session of the Open-Ended Working Group on security of and in the use of ICTs (2021-2025) - International Law*, UN, New York (4 December 2024).

UN General Assembly, *Report of the International Law Commission on the work of its fifty-second session*, A/CN.4/513 (15 February 2001).

- *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/201 (30 July 2010).
- *Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General*, A/66/152, A/66/152 (15 July 2011)
- *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).
- *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/70/174 (22 July 2015).
- *Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report*, A/AC.290/2021/CRP.2 (10 March 2021).
- *Chair's Summary of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/AC.290/2021/CRP.3 (10 March 2021).
- *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).

- Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, A/76/136* (13 July 2021).
 - 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).
 - 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).
 - 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).
 - Mapping exercise to survey the landscape of capacity-building programmes and initiatives within and outside the United Nations and at the global and regional levels, A/AC.292/2024/2 (22 January 2024).
 - Lethal autonomous weapons systems: Report of the Secretary-General, A/79/88 (1 July 2024).
 - Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, A/79/214 (22 July 2024).
 - Initial report outlining the proposal for the development and operationalization of a dedicated Global Information and Communications Technologies Security Cooperation and Capacity-Building Portal, A/AC.292/2025/1 (14 January 2025).
- UN, Fourth report on international liability for injurious consequences arising out of acts not prohibited by international law, by Robert .Q. Quentin-Baxter, Special Rapporteur, A/ CN.4/373 and Corr.1&.2 (27 June 1983).
- UNIDIR, A Compendium of Good Practices: Developing a National Position on the Interpretation of International Law and State Use of ICT (2024).

International treaties, resolutions and other documents

26th International Conference of the Red Cross and Red Crescent, Resolution 1: International Humanitarian Law – From Law to Action, 26IC/95/R1 (3 December 1995).

34th International Conference of the Red Cross and Red Crescent, Resolution 2: Protecting Civilians and Other Protected Persons and Objects Against the Potential Human Cost of ICT Activities During Armed Conflict, 34IC/24/R2 (October 2024).

African Charter on Human and Peoples' Rights, CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982) (27 June 1981).

American Convention on Human Rights, Treaty Series, No 36 (open for signature from 22 November 1969, entered into force 18 July 1978), 1144 UNTS 123.



Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS 16.

Convention on the Prevention and Punishment of the Crime of Genocide (signed 9 December 1948, entered into force 12 January 1951) 78 UNTS 277.

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, ETS 5 (4 November 1950).

Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (signed 12 August 1949, entered into force 21 October 1950) 75 UNTS 3.

Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (signed 12 August 1949, entered into force 21 October 1950) 75 UNTS 85.

Geneva Convention (III) relative to the Treatment of Prisoners of War (signed 12 August 1949, entered into force 21 October 1950) 75 UNTS 135.

Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War (signed 12 August 1949, entered into force 21 October 1950) 75 UNTS 287.

HRC, General Comment No 31 [80]: The nature of the general legal obligation imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13 (26 May 2004).

– General Comment No 34: Article 19: Freedoms of opinion and expression, CCPR/C/GC/34 (12 September 2011).

– General Comment No 36: Article 6: Right to Life, CCPR/C/GC/36 (3 September 2019) (General Comment 36).

ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, A/56/10 (2001).

– Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, A/56/10 (2001).

– Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties, A/73/10 (2018).

– Draft conclusions on the identification of customary international law, with commentaries, A/73/10 (2018).

– Draft articles on Prevention and Punishment of Crimes Against Humanity, A/74/10 (2019).

– Draft conclusions on identification and legal consequences of peremptory norms of general international law (jus cogens), A/77/10 (2022).

International Convention on the Elimination of All Forms of Racial Discrimination (21 December 1965) 660 UNTS 195.

International Covenant on Civil and Political Rights (16 December 1966) 999 UNTS 171.

OHCHR, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' (2011).



Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (signed 12 December 1977, entered into force 7 December 1978) 1125 UNTS 3.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (signed 12 December 1977, entered into force 7 December 1978) 1125 UNTS 609.

Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 90 (as amended).

Statute of the International Court of Justice, of 26 June 1945, annexed to the UN Charter.

UN General Assembly, Declaration on the Granting of Independence to Colonial Countries and Peoples, Res 1514 (XV) (14 December 1960).

– 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) (24 October 1970) Annex.

– Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, A/RES/36/103 (9 December 1981).

– Manila Declaration on the Peaceful Settlement of International Disputes, A/RES/37/10 (15 November 1982).

– Resolution adopted by the General Assembly on 22 December 2018 [on the report of the First Committee (A/73/505)] 73/266. Advancing responsible State behaviour in cyberspace in the context of international security, A/RES/73/266 (2 January 2019).

– Global Digital Compact, A/79/L.2 (22 September 2024).

– Artificial intelligence in the military domain and its implications for international peace and security, A/RES/79/239 (31 December 2024).

UN, Proclamation of Teheran, Final Act of the International Conference on Human Rights, Teheran, 22 April to 13 May 1968, A/CONF.32/41.

UNHRC, The promotion, protection and enjoyment of human rights on the Internet, A/HRC/RES/32/13 (1 July 2016).

Universal Declaration of Human Rights (UN General Assembly resolution 217 A (III) of 10 December 1948).

Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331.

International case-law

ECtHR, Banković and others v Belgium and others (App no 52207/99) (12 December 2001).

– Al-Skeini and others v United Kingdom (App no 55721/07) (7 July 2011).

IACtHR, Velásquez Rodríguez v Honduras, (Merits) (Ser C) No 4 (29 July 1988).



ICC, *Prosecutor v Ntaganda, Appeals Judgment on the appeals of Mr Bosco Ntaganda and the Prosecutor against the decision of Trial Chamber VI of 8 July 2019 entitled 'Judgment'* (30 March 2021), ICC-01/04-02/06-2666-Red 30-03-2021.

ICJ, *Corfu Channel Case (UK v Albania)* (Merits) [1949] ICJ Rep 4.

- *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US)* (Merits) [1986] ICJ Rep 14.
- *East Timor (Portugal v Australia)* (Judgment) [1995] ICJ Rep 90.
- *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226.
- *Gabčíkovo-Nagymaros Project (Hungary/Slovakia)* (Judgment) [1997] ICJ Rep 7.
- *Fisheries Jurisdiction (Spain v Canada)* (Jurisdiction of the Court) [1998] ICJ Rep 432.
- *Case Concerning Oil Platforms (Iran v US)* (Judgment) [2003] ICJ Rep 161.
- *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) [2004] ICJ Rep 136.
- *Case Concerning Armed Activities in the Territory of the Congo (Democratic Republic of Congo v Uganda)* (Merits) [2005] ICJ Rep 168.
- *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* (Judgment) [2007] ICJ Rep 43.
- *Pulp Mills on the River Uruguay (Argentina v Uruguay)* (Judgment) [2010] ICJ Rep 14.
- *Legal Consequences of the Separation of the Chagos Archipelago from Mauritius in 1965* (Advisory Opinion) [2019] ICJ Rep 95.

ICTY, *Prosecutor v Tadić* (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) ICTY-94-1-A (2 October 1995).

- *Prosecutor v Tadić* (Appeal Judgment) IT-94-1-A (15 July 1999).
- *Prosecutor v Limaj* (Trial Judgment) ICTY-03-66-T (30 November 2005).
- *Prosecutor v Boškoski and Tarčulovski* (Trial Judgment) ICTY-04-82-T (10 July 2008).

Island of Palmas (US v Netherlands) (1928) II RIAA 829.

Trail Smelter Case (US v Canada) (1941) 3 RIAA 1911.



ANNEX A:

Checklist for developing a national position

This checklist offers a non-exhaustive list of considerations that may assist States in developing or reviewing a national position on the application of international law to cyber activities. It is organised in line with the structure of the Handbook and is intended as a practical reference tool to help guide internal planning, coordination, and decision-making. Not all points will be relevant in every context and their sequence may need to be tailored to fit national requirements.

Motivations (for more information, see Chapter 2)

- ☐ Identify the principal motivations for developing a national position.
- ☐ Consider what functions the position should serve (e.g. communicative, transformative, preventative).
- ☐ Outline the respective aims and expected outcomes of the national position.
- ☐ Identify possible risks, constraints, or sensitivities, including those related to disclosure, operational flexibility, available capacity or lack of internal consensus.
- ☐ Decide whether to develop a national position.
- ☐ Consider whether to proceed with a public, partial, or internal-only position, and how best to manage strategic omissions if needed.

Process (for more information, see Chapter 3)

- ☐ Consider national specifics to tailor the process and the order of steps.
- ☐ Secure a mandate to initiate the process.
- ☐ Map relevant stakeholders across government and other sectors.
- ☐ Determine the lead agency and coordination mechanisms.
- ☐ Appoint one or more penholders and, if possible, a multidisciplinary drafting team.
- ☐ Develop a plan and timeline for the process, including major milestones. Consider using the 5W&H framework (*Who? What? Why? When? Where? How?*).
- ☐ Identify capacity-building needs and consider how these can be addressed (e.g. through partnerships, training, or external support).
- ☐ Consult relevant national and international stakeholders, including technical and operational agencies, legal advisors, and, where appropriate, the general public or civil society.

- ☐ Conduct desk research and gather reference materials from existing national positions, multilateral fora, academic sources, and domestic documents.
- ☐ Select a drafting approach (deductive, inductive, or hybrid).
- ☐ Draft the position through an iterative process, including an appropriate number of stages of internal review, consolidation, and refinement.
- ☐ Prepare for formal adoption in line with domestic legal or procedural requirements.
- ☐ Plan for future review, updates, or follow-up based on developments in law or policy.

Substance (for more information, see Chapter 4)

- ☐ Determine the desired breadth and depth of analysis, based on national interests and priorities.
- ☐ Consult existing national positions and other relevant resources such as the *Cyber Law Toolkit*, the *Oxford Process*, and the *Tallinn Manual 2.0*.
- ☐ Identify the key rules and principles of international law to be included (e.g. sovereignty, due diligence, non-intervention, prohibition of the use of force).
- ☐ Decide whether to include views on specialized regimes of international law (e.g. IHL, international human rights law, international criminal law).

Format and Dissemination (for more information, see Chapter 5)

- ☐ Choose an appropriate format (e.g. speech, submission to a multilateral forum, academic article, or standalone written document).
- ☐ Structure the document clearly and consider using headings, summaries, and numbered paragraphs.
- ☐ Determine the appropriate tone and level of technicality for the intended audiences.
- ☐ Consider including practical scenarios or real-world examples to illustrate key points.
- ☐ Review the consistency of terminology and framing across all topics.
- ☐ Ensure accessibility, including potential translations into other languages and the use of visual aids if relevant.
- ☐ Develop a dissemination strategy, including options for launch, such as a public event or online announcement.



ANNEX B:

List of common and national positions on international law and cyber activities

Common positions

1. African Union

Common position of the African Union (2024)

2. European Union

Common position of the European Union (2024)

National positions

1. Australia

National position of Australia (2017)

National position of Australia (2021)

2. Austria

National position of Austria (2024)

3. Brazil

National position of Brazil (2020)

National position of Brazil (2021)

4. Canada

National position of Canada (EN) (2022)

National position of Canada (FR) (2022)

5. China

National position of China (general) (2021)

National position of China (sovereignty) (2021)

6. Colombia

National position of Colombia (EN) (2025)

National position of Colombia (ES) (2025)

7. Costa Rica

National position of Costa Rica (2023)

8. Cuba

National position of Cuba (2024)

9. Czechia

National position of Czechia (2020)

National position of Czechia (2024)

10. Denmark

National position of Denmark (2023)

11. Estonia

National position of Estonia (2019)

National position of Estonia (2021)

12. Finland

National position of Finland (EN) (2020)

National position of Finland (FI) (2020)

13. France

National position of France (EN) (2019)

National position of France (FR) (2019)

National position of France (EN) (2021)



14. Germany

National position of Germany (2021)

15. Iran

National position of Iran (2020)

16. Ireland

National position of Ireland (2023)

17. Israel

National position of Israel (2021)

18. Italy

National position of Italy (2021)

19. Japan

National position of Japan (2021)

20. Kazakhstan

National position of Kazakhstan (2021)

21. Kenya

National position of Kenya (2021)

22. Netherlands

National position of the Netherlands (2019)

23. New Zealand

National position of New Zealand (2020)

24. Norway

National position of Norway (2021)

25. Pakistan

National position of Pakistan (2023)

26. Poland

National position of Poland (2022)

27. Romania

National position of Romania (2021)

28. Russia

National position of Russia (2021)

29. Singapore

National position of Singapore (2021)

30. Sweden

National position of Sweden (2022)

31. Switzerland

National position of Switzerland (2021)

32. United Kingdom

National position of the United Kingdom (2018)

National position of the United Kingdom (2021)

National position of the United Kingdom (2022)

33. United States

National position of the United States (2012)

National position of the United States (2016)

National position of the United States (2020)

National position of the United States (2021)



ANNEX C:

List of participating States

- | | |
|-----------------------------|---------------------------------|
| 1. Algeria | 24. Lesotho |
| 2. Angola | 25. Malaysia |
| 3. Argentina | 26. Mauritania |
| 4. Benin | 27. Mexico |
| 5. Brazil | 28. Morocco |
| 6. Burundi | 29. Mozambique |
| 7. Cambodia | 30. New Zealand |
| 8. Cameroon | 31. Paraguay |
| 9. Canada | 32. Peru |
| 10. Chile | 33. Philippines |
| 11. Colombia | 34. Republic of Korea |
| 12. Comoros | 35. Sahrawi Republic |
| 13. Congo (Republic of the) | 36. Senegal |
| 14. Côte d'Ivoire | 37. Singapore |
| 15. Dominican Republic | 38. South Africa |
| 16. Egypt | 39. South Sudan |
| 17. El Salvador | 40. Thailand |
| 18. Estonia | 41. Togo |
| 19. Ethiopia | 42. Uganda |
| 20. Gambia | 43. United Republic of Tanzania |
| 21. Indonesia | 44. United States of America |
| 22. Japan | 45. Uruguay |
| 23. Kenya | 46. Zambia |

Inclusion in this Annex reflects participation in the project roundtables and does not imply any recognition of legal status. Likewise, participation in the project does not constitute endorsement of the content of this Handbook.



ANNEX D:

List of project events

2024

Launch of the project 'The Handbook on Developing a National Position on International Law in Cyberspace: A Practical Guide for States', 16th International Conference on Cyber Conflict: Over the Horizon (CyCon 2024), 28 May 2024, Tallinn.

Panel: 'Navigating Legal Dynamics: National Perspectives on International Law and Potentials for Convergence', Third Annual In-Person Symposium on Cyber & International Law, Future Conflict: The International Law of Cyber and Information Convergence, American University, 24 September 2024, Washington, DC.

Roundtable on Developing National Positions on International Law in Cyberspace: Latin American and Caribbean Perspectives, Headquarters of the Organization of American States, 25–26 September 2024, Washington, DC.

Panel: 'National Positions on International Law in Cyberspace: Challenges, Opportunities, and Best Practices', Singapore International Cyber Week, 15 October 2024, Singapore.

Roundtable on Developing National Positions on International Law in Cyberspace: Asia & the Pacific Perspectives, Centre for International Law (CIL), National University of Singapore, 16 October 2024, Singapore.

Roundtable for African Union Member States on Developing a National Position on International Law in Cyberspace, African Union Headquarters, 25–26 November 2024, Addis Ababa.

2025

Launch of the *Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States*, 17th International Conference on Cyber Conflict: The Next Step (CyCon 2025), 29 May 2025, Tallinn.





