Madam Chair, Members of the Committee of Legal Advisers on Public International Law, Ladies and Gentlemen,

It is a true honor and a pleasure for me to address the 69th meeting of the Committee of Legal Advisers on Public International Law of the Council of Europe (CAHDI). On behalf of my fellow co-authors, I want to thank you for the invitation to present our recently published work, the **Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States**.

In 2015, the United Nations General Assembly adopted resolution A/RES/70/237 on the report of the First Committee concerning developments in the field of information and telecommunications in the context of international security. The resolution welcomed the conclusion that international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful, and accessible information and telecommunications environment. The key question became "how does international law apply?"—and states were repeatedly invited to voluntarily share their national views and positions, which may include national statements and State practice, on how international law applies to the use of information and communication technologies (ICTs).

Some States have been doing so from as early as 2012; however, a clear trend can be observed from about 2018–2019 and later. Today, 35 States and 2 international organizations have issued such statements in some form, with some having multiple ones (see collection in the CyberLaw Toolkit at **https://cyberlaw.ccdcoe.org**).

When we began this project in 2023, we recognized that the core challenge for many states wasn't a lack of interest, but a lack of a clear, structured methodology and practical guidance. The legal frameworks are complex, the technical realities are often obscure, and the political stakes are incredibly high. Therefore, developing a comprehensive and consistent position about where the legal boundaries lie in the complex and interconnected digital environment is non-trivial. National positions are carefully crafted since they have real-world impact.

Guidance and Content of the Handbook

This Handbook provides practical guidance for States developing or reviewing their national positions. It draws on insights from 46 States that participated in regional roundtables held in Addis Ababa, Singapore, and Washington, DC in 2024, alongside original research conducted for this project. The Handbook explores 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. 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. The Handbook also includes a concise **two-page checklist** that outlines key steps and best practices.

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 benefited from the support of partner institutions, including the **African Union, the Organization of American States, the Federal Foreign Office of Germany, the Centre for International Law at the National University of Singapore, and the Tallinn University of Technology.**

The Handbook and related resources **are available free of charge digitally** in the CCDCOE Library at **ccdcoe.org**; please also see the displayed QR code. Soon we are also launching explainer videos for each chapter.

Key Takeaways and Functions

What have we learned during the discussions and the project? The project team designed a set of questions that were used in all three roundtables and asked participants about: the importance and legal implications of national positions; the legal and policy considerations underlying a national position; the process of developing a national position; substantive issues covered in a national position; and format, style, and language choices for national positions.

National positions serve three main functions:

- Communicative function: Engaging with both domestic and international stakeholders.
- Transformative function: Clarifying and adapting the legal frameworks to new realities.
- Preventative function: Reducing the risk of misinterpretation while shaping assessments of violations and appropriate responses, thereby fostering deterrence.

The following quotes taken from the roundtables (under Chatham House Rules) well illustrate that cyber is not just a technical domain, but it is perceived as central to sovereignty, security, and development:

- "Articulating a national position on international law has consequences in real life and influences States' conduct, how States project power and react to projection of power, in and through Cyberspace."
- 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."
- "Drawing the line between legal and illegal behavior for itself and others, thus the prospect of legal consequences is a factor for ensuring restraint and respect for a State’s rights."
- "By clarifying the application of existing rules States begin to develop shared expectations and define the legal boundaries of how they should behave in Cyberspace."

Risks of Silence and Legal Valence

When participants were asked about why they develop a national position, they often were concerned with the consequences of not having a position, which was perceived as a less desirable state. For example, they were concerned that non-state actors could fill the gaps, or about the Global North driving the narrative, which may lead to systemic changes disfavouring the Global South/Global Majority, potentially also posing a risk to the systemic integrity of international law. "It is important to have as many voices heard as possible, so the minority of voices are not perceived as the majority." It was explained that there are risks associated with being silent (or omitting issues), including, for example, the risk of misinterpretation, both in internal and external contexts. Partial silence or omissions risk that domestic stakeholders read new meanings into the gaps. Thus, the benefit of developing a national position is the clarification of roles and preparedness in a crisis. Externally, silence risks, for example, a situation being read as acquiescence where not intended, and experts cautioned against assumptions regarding silence.

Some contrasted 'lawmakers' versus 'lawtakers' in this context, and pointed out that cyber provides a unique opportunity to be proactive—somewhat unlike in other domains where a conservative approach dominates when it comes to international law.

On that point, it is notable that the practice of developing such comprehensive national positions is not observed in other domains; this appears to be specific to cyber so far. Having a national position on narrower issues is certainly not new—it is routinely done. However, what is new is the breadth and scope that such positions cover: potentially the entire spectrum of international law.

This complexity poses many challenges, including how to organize the process; what is the understanding about the legal status of national positions; how to build the necessary capacity; how to decide what to include and what to omit in a national position; whether to publish it; and, if yes, in what format and how.

While all of these issues are important, I would like to address two issues that go beyond what is included in the Handbook: 1) legal status (valence) and 2) underrepresented topics.

1) Legal Valence

The overwhelming majority of participants and experts agreed that national positions have some legal weight. This is, of course, valid for statements that are formulated with the necessary language and precision, not necessarily for entire national position documents as such. On the other hand, there was a suggestion that since these positions are "living documents" and expected to evolve and change, they cannot have a binding effect.

When participants were asked to explain how exactly national positions can be binding, the responses differed significantly. Very few suggested these documents may be legally binding as unilateral acts giving rise to international legal obligations for the issuing state.

Many found it plausible that national positions may be understood as interpreting treaty law (VCLT Art 31(3)), since clearly there are references to specific treaty rules in national positions, e.g., UN Charter Article 2(4), various rules of the Geneva Conventions and Additional Protocols, etc.

Similarly, it was clear that theoretically, national positions (specific statements therein) may amount to *opinio juris* for the purposes of establishing or confirming the existence of customary international law. For example, "[I]n Poland's view, 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" [1].

However, experts were divided whether such national positions can amount to State practice, which would result in "double-counting."

One expert suggested on the legal status of national positions that perhaps we can view them as something between *opinio juris,* State practice, and interpretation of international law/interpretative aid. For different States, issuing a national position serves different purposes, and this can be stated in the position itself. This suggestion is slightly short of saying that national positions are *sui generis* in nature.

2) Underrepresented Topics

Participants were asked what topics, in their opinion, are underrepresented in existing national positions, and they pointed to the following (in random order):

- Peaceful settlement of disputes
- Due diligence
- Human rights
- Self-determination
- Law of neutrality
- Data embassies
- Data as an object under IHL
- Evidence
- Compensation (Art. 27(b) ARSIWA)

Conclusion

In conclusion, key takeaways are that there is significant divergence among the 100+ states which have either individually or in common positions expressed their views on how international law applies to cyber activities. As to the motivations, processes, substance, and presentation, there is no absolute methodology; there is no one-size-fits-all solution.

The need for tailoring the approach of each state and the complexity of the issue highlights the importance of capacity building in this area, both in terms of technical capacity building, but also in terms of international (cyber) law. While convergences and divergences exist in national positions, which may be perceived as discouraging or counterproductive, this is not new in international law, but a feature (see, e.g., treaty memberships). Developing a national position is a sovereign decision, but it contributes to improved clarity on what is the expected behavior in cyberspace, thereby fostering predictability. These positions are a sign that even if legal differences and geopolitical tensions remain, constructive dialogue is possible.

Finally, as one participant said: "What happens in Cyberspace does not stay in Cyberspace!" Cyberspace activities have real-life consequences. But also, national positions address questions of international law generally, not only cyber-specific ones. Therefore, these national positions and the developments in this field may have a broader impact and spill over the boundaries of the current discussions.

Thank you very much, and I am standing by for your questions.

CCDCOE

NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

DISCLAIMER

The views expressed in this presentation are those of the author in his/her personal capacity and should not be understood to necessarily represent those of the NATO Cooperative Cyber Defence Centre of Excellence or any NATO entity.

The Handbook on Developing a National Position on the Application of International Law and Cyber Activities

CAHDI, 25.09.2025, Strasbourg

Dr Agnes Kasper, co-author of the Handbook

CCDCOE

Agnes Kasper, PhD

Head of Law Branch

NATO CCDCOE, Tallinn, Estonia – Head of Law Branch

Tallinn University of Technology, Dept. of Law, Estonia – Senior Lecturer

- Ph.D. Multi-level analytical frameworks for cyber security legal decision making (2015)
- MA in Law
- BA International Business

Held positions at human rights organizations, embassies, private IT consultancy companies

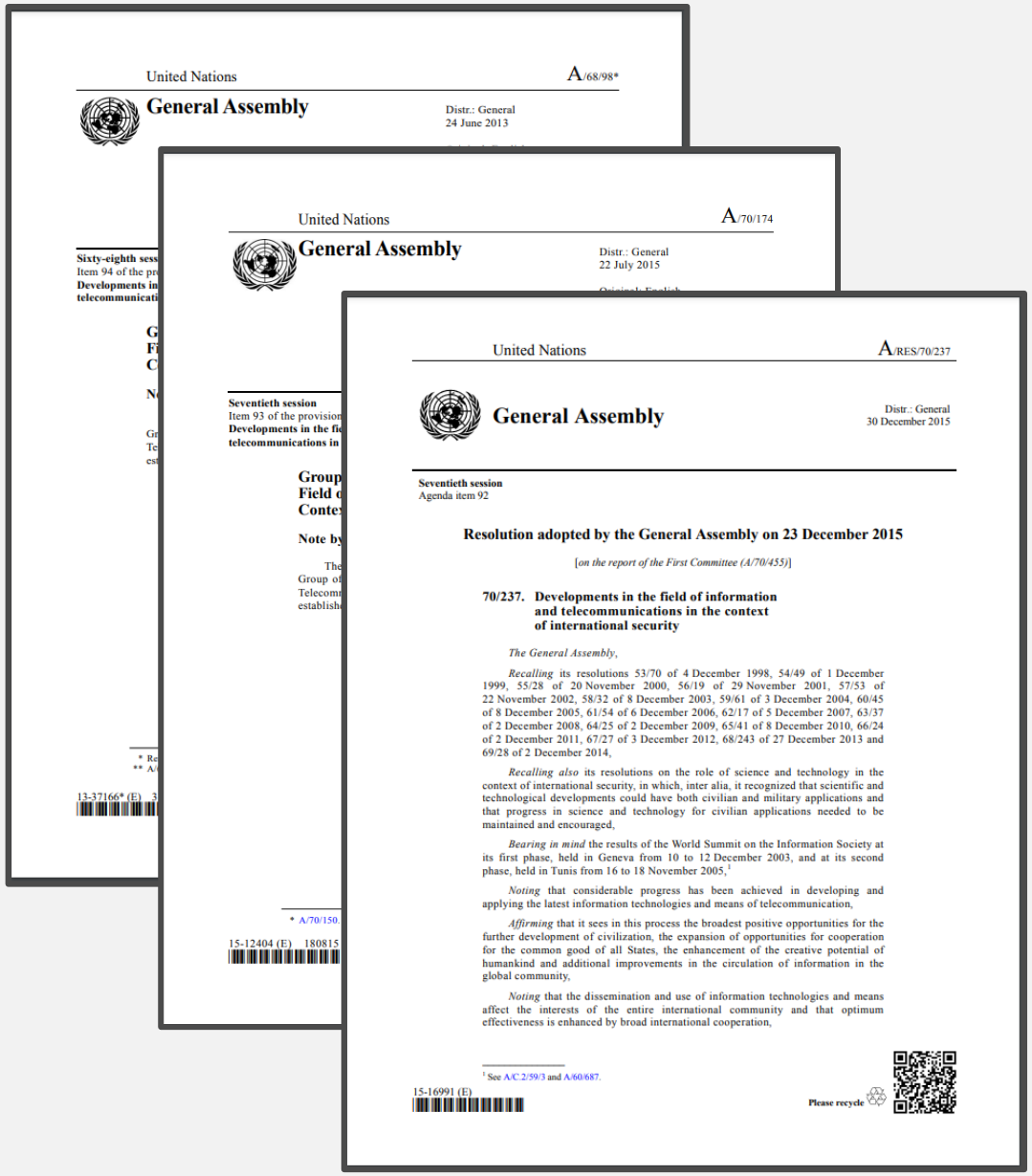
Agnes Kasper, PhD
Head of Law Branch
NATO CCDCOE
ph: +372 717 6804
mob: +372 5265 221
agnes.kasper@ccdcoe.org

CCDCOE

Consensus on Intl' law and cyber

19. **International law, and in particular the Charter of the United Nations, is applicable** and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.

20. State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.



CCDCOE

National positions are statements where States articulate their positions on **how**, in their view, international law applies to conduct of cyber activities.

CCDCOE

State positions on HOW international law applies in cyberspace

Common positions

Edit | Edit Source

- African Union (2024)
- European Union (2024)

National positions

Edit | Edit Source

- Australia (2020)
- Austria (2024)
- Brazil (2021)
- Canada (2022)
- China (2021)
- Colombia (2025)
- Costa Rica (2023)
- Cuba (2024)
- Czech Republic (2020 and 2024)
- Denmark (2023)
- Estonia (2019 and 2021)
- Finland (2020)
- France (2019)
- Germany (2021)
- Iran (2020)
- Ireland (2023)
- Israel (2020)
- Italy (2021)
- Japan (2021)
- Kazakhstan (2021)
- Kenya (2021)
- Netherlands (2019)
- New Zealand (2020)
- Norway (2021)
- Pakistan (2023)
- Poland (2022)
- Romania (2021)
- Russia (2021)
- Singapore (2021)
- Sweden (2022)
- Switzerland (2021)
- United Kingdom (2018, 2021 and 2022)
- United States (2012, 2016, 2020 and 2021)

CCDCOE

Cyber Law Toolkit

'BRIDGING THE GAP BETWEEN ACADEMIA AND PRACTICE'

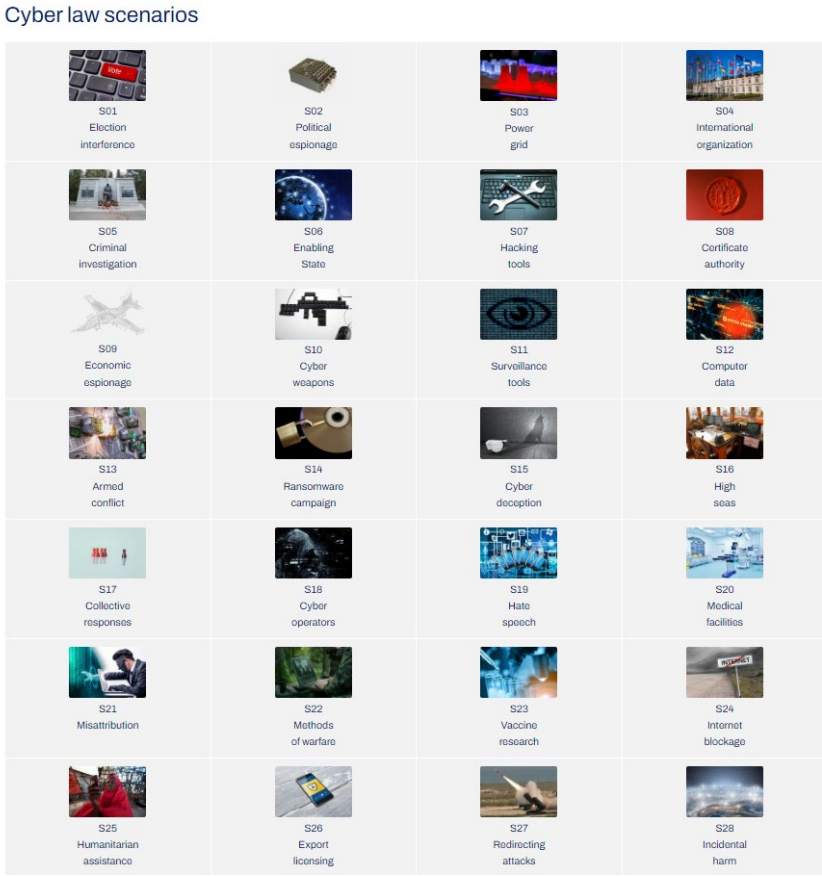
WHAT: Interactive web-based tool, no fee, continuously updated, externally peer-reviewed

WHO: For those working on/interested in international law and cyber operations

HOW: Hypothetical scenarios based on real-life examples

- → Facts + international law analysis
- → Featured incidents – cyber incidents summaries
- → ***National positions on application of international law***
- → Multiple search functions (scenarios, key word cloud, full text search, FAQ, list of articles)

https://cyberlaw.ccdcoe.org



CCDCOE

It is **non-trivial** to develop a comprehensive and consistent position about where the **legal boundaries** lie in the complex and interconnected digital environment.

These national positions are carefully **crafted** since they have real-life impact.

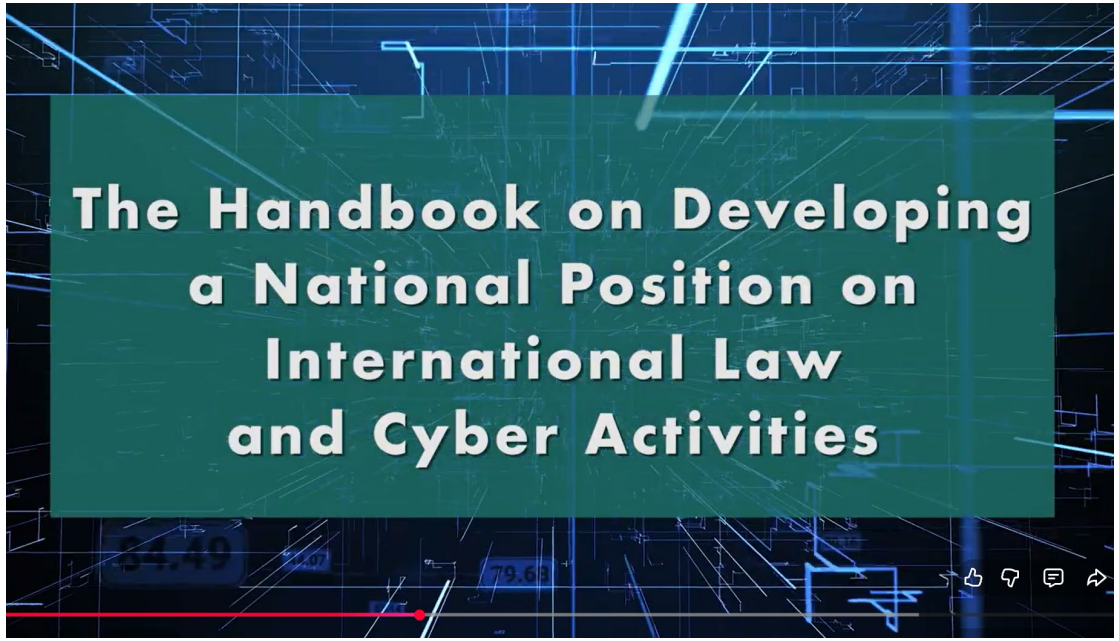
Handbook on Developing a National Position on International Law and Cyber Activities 2025

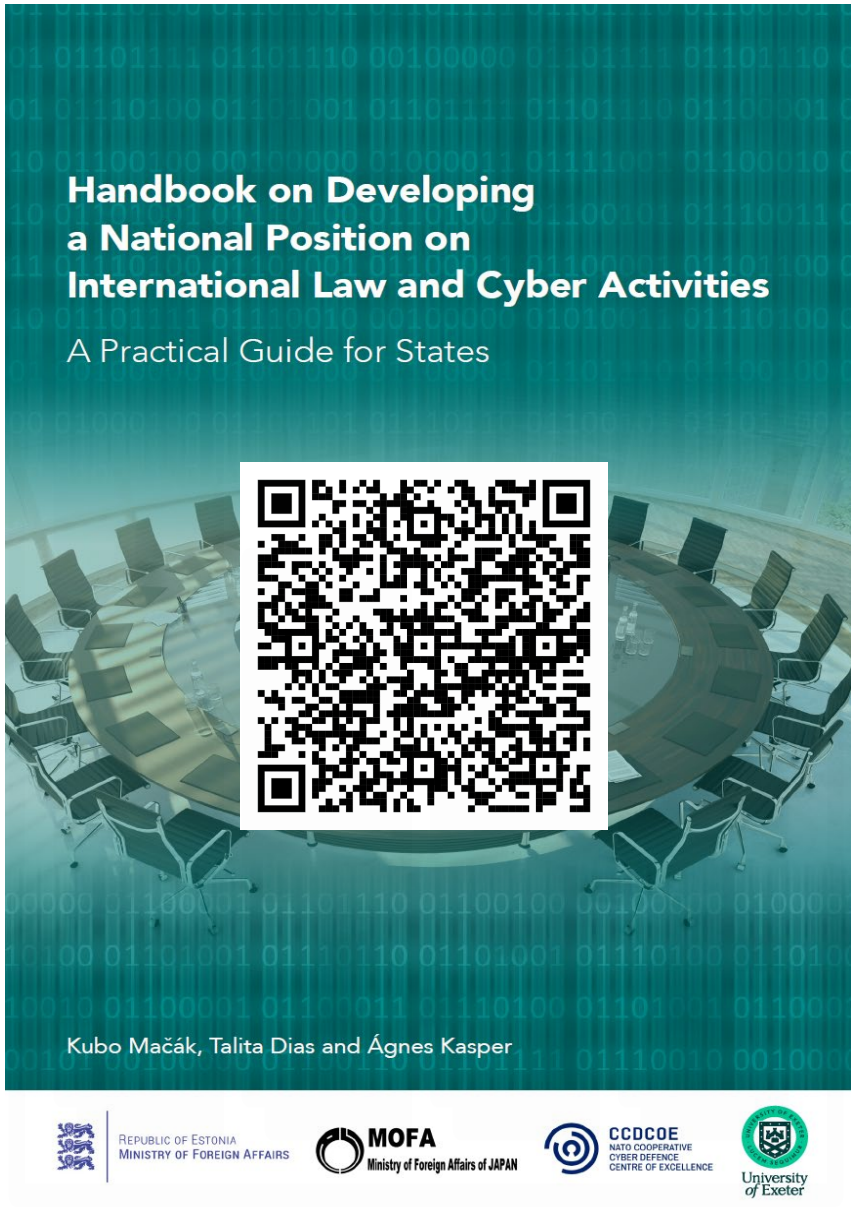
- **Practical guidance**: Substantive, procedural, policy questions facing nations when developing their positions on how international law applies in cyberspace
- Partners: University of Exeter, NATO CCDCOE, Japan MFA, Estonia MFA
- 3 editors/co-investigators: Prof Kubo Mačák; Dr Talita Dias; Dr Agnes Kasper
- 3 closed roundtables, 4 continents, 46 States, 77 officials
- UN Launch on 8th July 2025 at OEWG final session, NY

Avalilable free of charge digitally in the [CCDCOE Library]

CCDCOE

Related resources





CCDCOE

Functions of National positions

- Communicative function, **engaging** with domestic and international stakeholders;
- Transformative function, **clarifying and adapting legal** frameworks to new realities (new interpretations and/or customary law may be emerging as more national positions are published);
- Preventative function, **reducing the risk of misinterpretation** while shaping assessments of violations and appropriate responses, thereby fostering **deterrence**.

CCDCOE

Importance of national positions

*„Articulating a national position on international law has consequences in real-life and influence States conduct, **how States project power and react to projection of power**, in and through Cyberspace“;*

*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**“;*

*„Drawing the **line between legal and illegal behaviour for itself and others**, thus the prospect of **legal consequences** is a factor for ensuring restraint and respect for a State's right“;*

*„By **clarifying the application of existing rules** States begin to develop shared expectations and **define the legal boundaries** of how they should behave in Cyberspace“;*

*„Re-shape the **dynamics of international relations** in the digital environment“.*

Roundtable participants and project experts

CCDCOE

Handbook overview

Introduction	• National positions and their significance
Motivation	• Why would a State decide to develop a national position?
Process	• How does a State develop a national position?
Substance	• Which issues and topics might a national position include?
Presentation	• How might a national position be presented?
Conclusion	• What comes next?
Bibliography & Annexes	• Bibliography, Checklist, List of Documents, Events, Participating States

CCDCOE

KEY TAKEAWAYS

- ✓ **35 national and 2 common positions = 100+ countries - *No one-size-fits all*!**
- ✓ **Capacity-building in international (cyber) law is of high importance**
- ✓ **Convergences and divergences - that's not new in internatonal law, but rather a feature**
- ✓ **„What happens in Cyberspace, does not stay in Cyberspace!“**

OUTLINE OF HANDBOOK CHAPTERS

Chapter 1. Introduction

National positions included in the Handbook:

- → Issued publicly
- → Issued by a State organ
- → Available in a written format in a public repository
- → Published with the aim of expressing specific legal views on the application of international law in the cyber context

Chapter 1. Introduction

Legal significance:

National positions carry some degree of legal valence

- → Unilateral acts giving rise to int'l legal obligations for the issuing state?
- → Interpret treaty law
- → Affirm (or reject) customary nature of rules
- → *Opinio juris* & state practice?
- → Silence?

CCDCOE

Chapter 2. Motivations

Why to develop a national position?

Overall factors:

- → External and internal policy considerations and drivers (motivate the deployment of …)
- → Communicative, transformative and preventative functions (to achieve…)
- → Explicit or implicit aims, desired outcomes, future-oriented goals

Chapter 2. Motivations

Specific aims and motivations (with inherent overlaps):

- → Preventing miscalculation and escalation – increasing predicatability and stability at scale
- → Enhancing compliance and accountability – deterring and preventing violations
- → Shaping the evolution of international law – addressing legal uncertainty
- → Improve domestic frameworks for action and increase cyber resilience

Chapter 2. Motivations

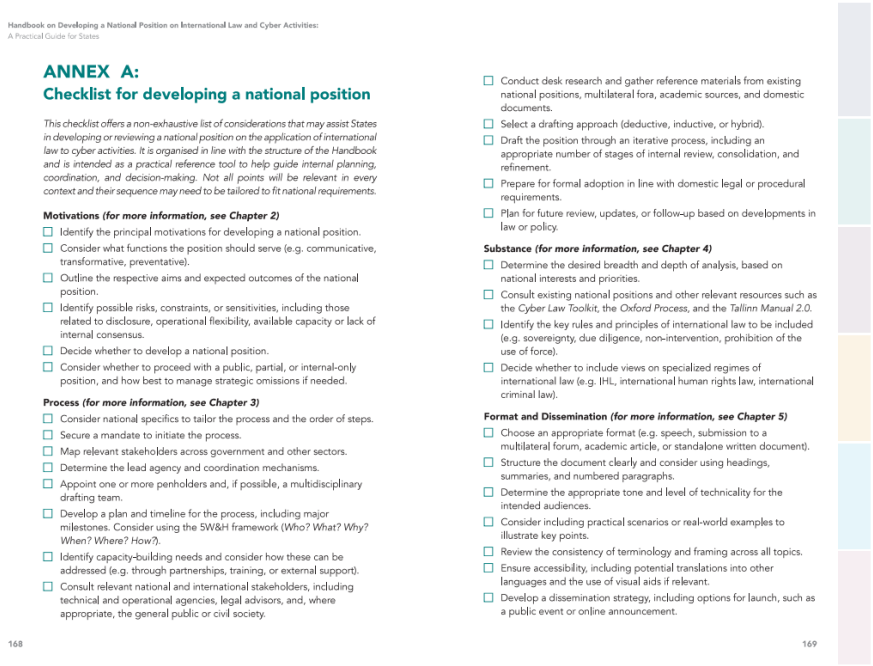
Constraining factors:

- → Lack of capacity
- → Absence of political will
- → Non-disclosure
- → Strategic omissions
- → Maintaining policy and operational flexibility
- → Lack of consensus

Chapter 3. Process

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.

- Comprehensiveness, complexity and novel expectations
- Mix of steps and techniques used in public policy processes and methodologies of international law
- Checklist included in Annex A.



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.

CCDCOE

Chapter 3. Process

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

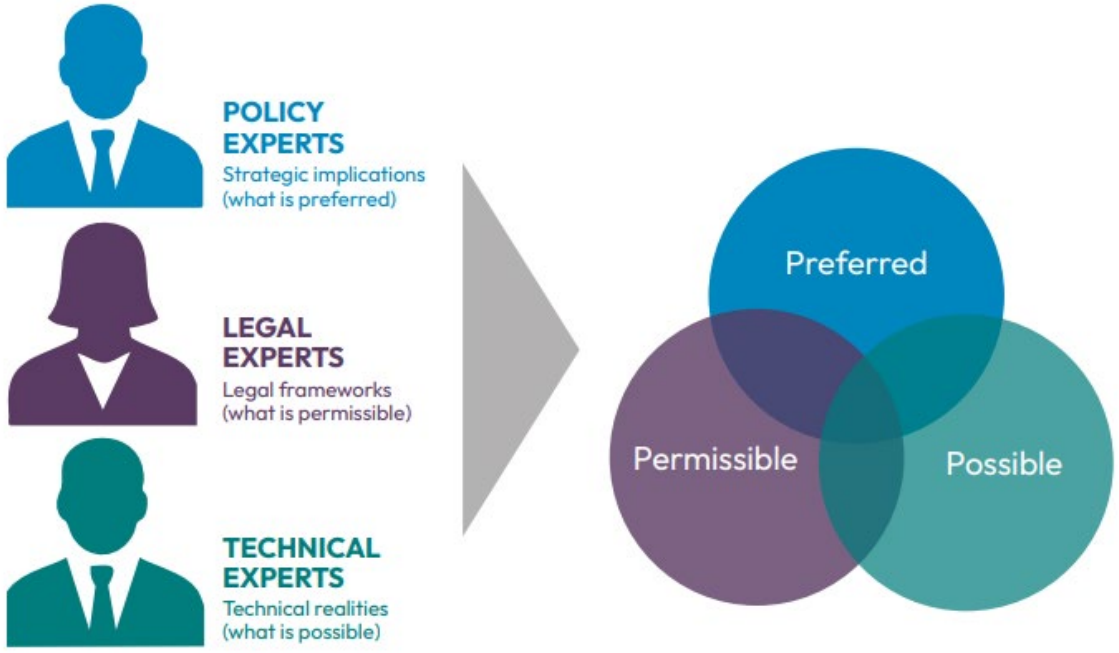


Figure 2: Composition of the drafting team.

CCDCOE

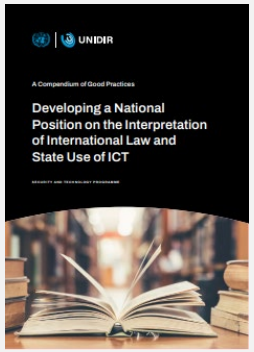
Chapter 3. Process

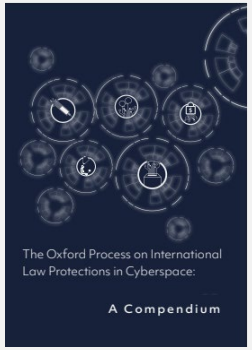
Preparations and planning

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.

Capacity-building

UN Capacity-building principles





CCDCOE

Chapter 3. Process

Research, analysis and drafting

Sources to use, eg.:

- National positions
- Documents from dedicated UN fora and expert groups
- Other UN sources
- Cyber-specific academic sources
- Documents from international organizations
- Sources of international law
- National legislation and policies
- Etc.

- Elimination approach
- Inclusion approach

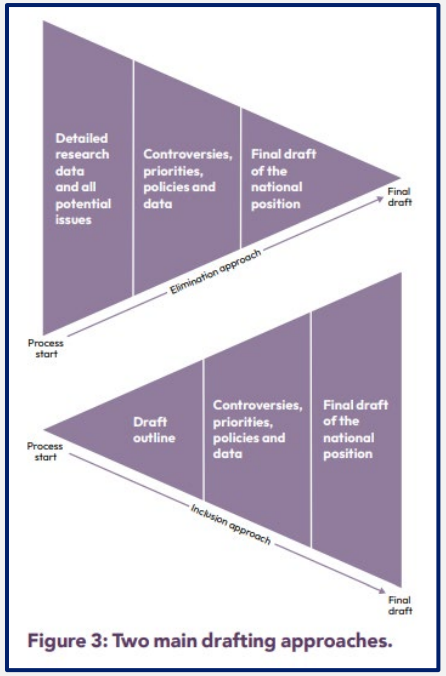


Figure 3: Two main drafting approaches.

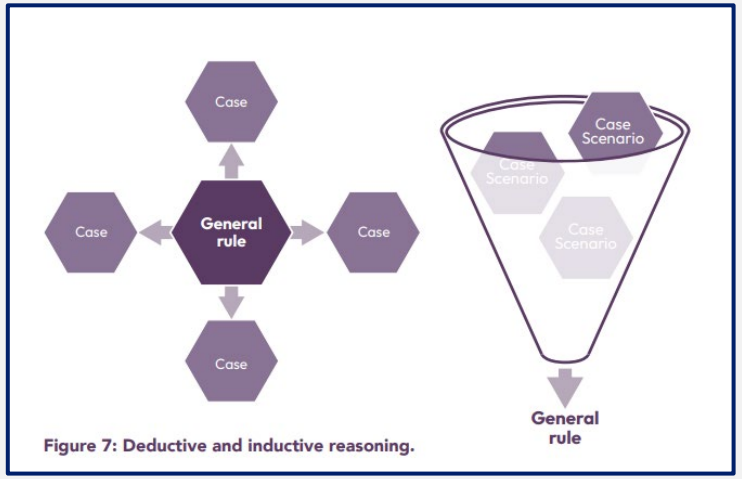


Figure 7: Deductive and inductive reasoning.

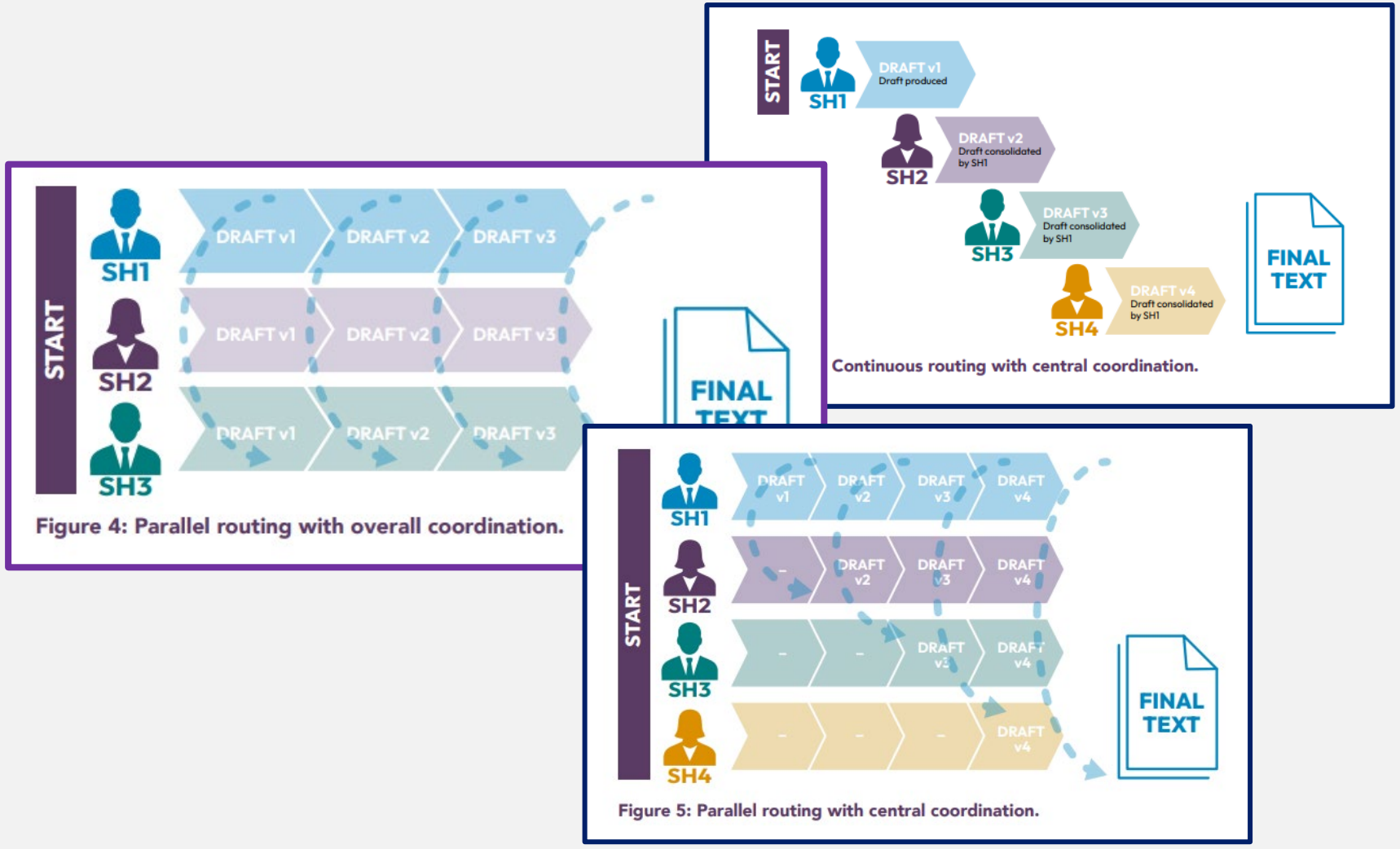
- Deductive reasoning
- Inductive reasoning

CCDCOE

Chapter 3. Process

Consultation models

- Parallel
- Continuous



CCDCOE

Chapter 3. Process

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**.

CCDCOE

Chapter 4. Substance

The existing national positions on international law and cyber activities cover a wide range of substantive issues.

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. National positions address the following broad areas:

- Foundational rules and principles
- Specialized regimes
- State responsibility

CCDCOE

Chapter 4. Substance

Foundational rules and principles

Sovereignty

- Rule/principle
- Access/effects
- Cyber espionage

Non-intervention

- *Domaine réservé*
- Coercive intent/effect

Due diligence

- Prevention & no-harm principle
- Rule/principle
- Conduct/result

Use of force

- 'Force'
- Threshold
- Armed attack

Peaceful settlement of disputes

- Scope
- Choice of means
- Factual/legal disputes

Self-determination

- Collective right
- Internal/external
- Potential norms conflict

CCDCOE

Chapter 4. Substance

Specialized regimes

Law of Armed Conflict	International Human Rights Law	International Criminal Law
• Applies in cyber • IAC/NIAC • IHL principles • 'Attack' (Art 49 AP I) • Data as an object	• High relevance • Jurisdiction • Absolute & qualified rights • Interference reqs.	• Core intl' crimes • Customary & treaty law • Cyber-enabled • Principle of legality

CCDCOE

Chapter 4. Substance

State responsibility (customary law)

Attribution	Countermeasures	Necessity
• State organs • Non-state actors • Threshold • Reasonably substantiated	• Precluding wrongfulness • Substantive reqs. • Procedural reqs. • Collective	• Precluding wrongfulness • Grave & imminent peril against essential state interest (incl. non-physical harm) • No prior IWA

CCDCOE

Chapter 5. Presentation

Presentation affect clarity, reach and impact

It is about format, length, structure, language, use of examples, dissemination, etc.

CCDCOE

Chapter 5. Presentation

Format & style

- Oral/written
- Length
- Scenarios & examples
- References
- Headings, summaries, numbered paras
- Visual aids

Language

- Legal terminology
- Language of publication and translation

Dissemination

- Formal channels
- OEWG Document database
- Academic articles
- Blogs
- Visibility and accessibility

CCDCOE

Chapter 6. Conclusion

Mapping out areas of convergence, divergence and possible gaps

Full alignment is virtually impossible and may not even be desirable

States better understand their differences, can constructively debate them, striving for common grounds

Raise awareness and extend discussions to other regions

More in-depth discussions in international and domestic forums, possibly through scenario-based excercises and case studies

Model of national positions can be leveraged to foster dialogue and common understandings on other global challenges

CCDCOE

Chapter 6. Conclusion

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.

CCDCOE

Bibliography & Annexes

- Bibliography
- Annex A: Checklist for developing a national position
- Annex B: List of common and national positions on international law and cyber activities (as of May 2025)
- Annex C: List of participating States
- Annex D: List of project events

CCDCOE

Acknowledgements

The 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 initiative was funded by a £75,000 grant through the UK Economic and Social Research Council's Impact Accelerator Account.

The project has also benefitted from the support of partner institutions including the African Union, 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.

CCDCOE

Thank you!

CCDCOE

ccdcoe.org
@ccdcoe