



UNIDIR

Unpacking Cyber Capacity-Building Needs

Part I. Mapping the Foundational Cyber Capabilities

SAMUELE DOMINIONI · GIACOMO PERSI PAOLI



Acknowledgements

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This study is part of UNIDIR's Security and Technology Programme cyber workstream, which is funded by the Governments of Czechia, France, Germany, Italy, the Netherlands, Switzerland, and the United Kingdom, and by Microsoft.

About UNIDIR

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

Note

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

Authors



Samuele Dominioni

Researcher, Security and Technology Programme

Dr. Samuele Dominioni is a researcher in the Security and Technology Programme at UNIDIR. Before joining UNIDIR, he held research positions in both academic and think tank settings. He holds a PhD in international relations and political history from Sciences Po, France, and the IMT School for Advanced Studies, Italy.



Giacomo Persi Paoli

Head of Programme, Security and Technology

Dr. Giacomo Persi Paoli is the Head of the Security and Technology Programme at UNIDIR. His expertise spans the science and technology domain with emphasis on the implications of emerging technologies for security and defence. Before joining UNIDIR, Giacomo was Associate Director at RAND Europe where he led the defence and security science, technology and innovation portfolio as well as RAND's Centre for Futures and Foresight Studies. He holds a PhD in Economics from the University of Rome, Italy, and a Master's degree in political science from the University of Pisa, Italy.

Contents

- Abbreviations and Acronyms** **5**
- Executive Summary** **6**

- 1. Introduction** **8**
 - A Note on Methodology 10

- 2. Introducing Foundational Cyber Capabilities** **11**

- 3. Unpacking FCCs: Norms of Responsible State Behaviour** **14**
 - 3.1 Norm A 16
 - 3.2 Norm B 19
 - 3.3 Norm C 21
 - 3.4 Norm D 23
 - 3.5 Norm E 25
 - 3.6 Norm F 27
 - 3.7 Norm G 28
 - 3.8 Norm H 30
 - 3.9 Norm I 32
 - 3.10 Norm J 34
 - 3.11 Norm K 36

- 4. Unpacking FCCs: International Law** **38**

- 5. Unpacking FCCs: Confidence-Building Measures** **40**

- 6. Conclusions** **42**

- Annex 1. Foundational Cyber Capabilities Table** **44**

Acronyms & Abbreviations

CBM	Confidence-Building Measures
CERT/CSIRT	Computer Emergency Response Team/Computer Security Incident Response Team
CVD	Coordinated Vulnerability Disclosure
FCC	Foundational Cyber Capabilities
GGE	Group of Governmental Experts
ICT	Information Communication Technology
OEWG	Open Ended Working Group
UNIDIR	United Nations Institute for Disarmament Research
UNODA	United Nations Office for Disarmament Affairs
VEX	Vulnerability Exploitability Exchange


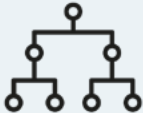





Executive Summary

Over the past two decades, States have been actively exploring ways of ensuring international peace and security in the domain of Information and communication technologies (ICTs). These efforts resulted in the adoption by the General Assembly of a set of measures that collectively are referred to as the Framework for Responsible State Behaviour in cyberspace (henceforth the Framework) that elaborates on what Members States should and should not do in the ICT environment from an international security perspective. The Framework is based on the components underpinned by targeted capacity-building: 11 voluntary, non-binding norms of responsible State behaviour, confidence-building measures and international law.

In the ongoing OEWG (2021–2025), many Member States have emphasized the need to support the implementation of the Framework, including through dedicated guidance, assistance and dedicated capacity-building efforts. This report is the first part of a study undertaken by UNIDIR to support States in their efforts to implement the Framework and to increase their cybersecurity and resilience.

In particular, this report identifies *foundational cyber capabilities* (FCCs) defined as the combination of policies and regulations, processes and structures, partnerships and networks, people and skills, and technology considered necessary to implement each element of the Framework: the 11 norms, international law and confidence-building measures.

<p>Policies and Regulations</p> 	<p>Official documents related to cybersecurity matters. These include documents outlining Member States' positions, policies, strategies (developed specifically for key sectors, e.g. critical infrastructure, or for national-level cross-sector applications), legal and regulatory frameworks, and signatures of agreements or other forms of cooperation with international stakeholders.</p>
<p>Processes and Structures</p> 	<p>Key positions, responsible agencies/entities, other national or regional mechanisms, and official processes, procedures and protocols related to cybersecurity.</p>
<p>Partnerships and Networks</p> 	<p>Initiatives both at the domestic and international level aimed at strengthening national capacity. At the domestic level, it includes mechanisms or instruments for intrasectoral and intragovernmental cooperation. At the international level, mechanisms, or instruments for bilateral, regional, and multilateral cooperation.</p>
<p>People and Skills</p> 	<p>Knowledge and expertise related to cybersecurity. It should be noted that certain FCCs listed under the 'people and skills' pillar could be met also by outsourcing and establishing agreements with external providers or other stakeholders, should the State not be able to develop or sustain this specialized capability internally.</p>
<p>Technology</p> 	<p>National-level technical solutions/capabilities pertaining to cybersecurity. It should be noted that the FCCs listed under the 'technology' pillar could be met also by outsourcing to external service providers through, for example, public-private partnerships.</p>

It is important to note that the FCCs are intended to serve as a baseline upon which more refined and comprehensive responses could be developed once such a baseline is met. FCCs therefore represent 'minimum' capability requirements necessary for the implementation of the Framework, not the best solutions or 'optimal' capability requirements.

The set of FCCs can be used as a tool to support better identification of requirements and better prioritization of capacity-building interventions, based on specific national needs and contexts, thus reinforcing the links between the implementation of the Framework and the discussions related to capacity-building, including those occurring in the current OEWG (and potential future Programme of Action).



1. Introduction

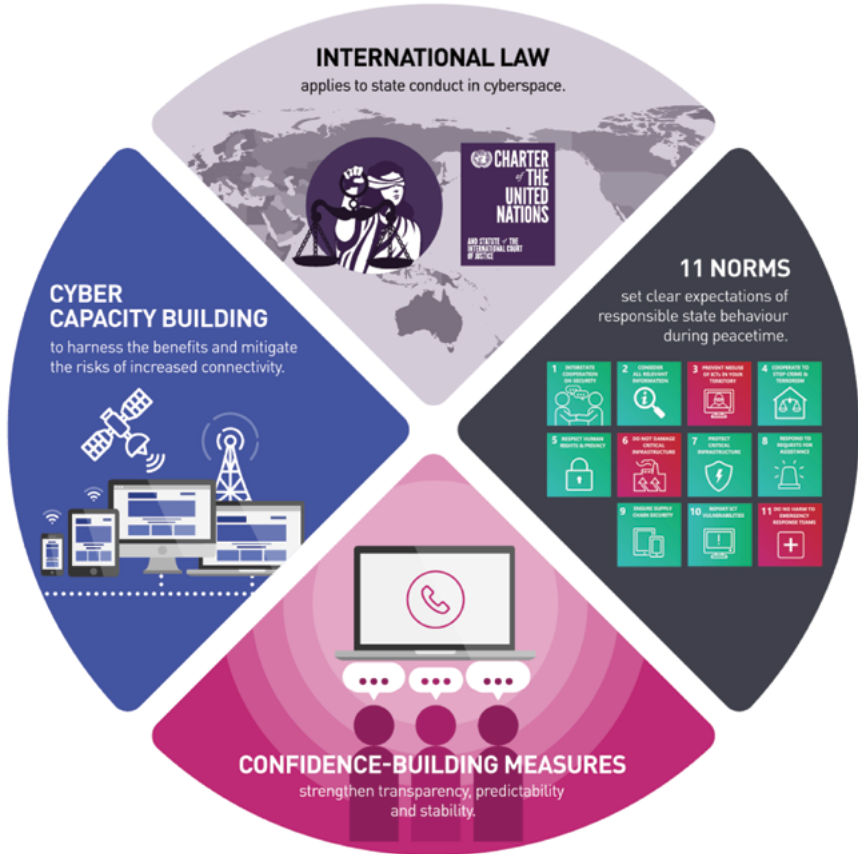
The information and communication technologies (ICTs) domain has changed and evolved throughout the decades, and it has expanded to cover almost all of the different facets of human activities. The United Nations recognized that nowadays ICTs “have implications for [...] peace and security, human rights and sustainable development. ICTs and global connectivity have been a catalyst for human progress and development, transforming societies and economies, and expanding opportunities for cooperation”.¹ Along with this growing relevance of ICTs in different sectors, in the last decades there have also been multiple attempts to set regulatory frameworks for the ICT domain.

Among these efforts to regulate the ICT domain, there is the Framework for Responsible State Behaviour (henceforth the Framework) that elaborates on what Member States should and should not do in the ICT environment from an international security perspective. The Framework is the result of around two decades of negotiations (in different formats) at the United Nations. In particular, it is based on the report of the 2021 Open-ended Working Group (OEWG) on developments in the field of ICTs in the context of international security and the consensus reports of the 2010, 2013, 2015, and 2021 Groups of Governmental Experts (GGEs).

1 [OEWG. 2021. Final Substantive Report](#), para 2.

In these reports, which are cumulative in nature, Member States developed 11 voluntary, non-binding norms of responsible State behaviour, recommended specific confidence-building, capacity-building and cooperation measures, and that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment. These three elements (norms, international law and confidence-building measures), underpinned by capacity-building, form the Framework (see figure 1).

Figure 1. The United Nations Framework for Responsible State Behaviour in Cyberspace



Source: <https://www.internationalcybertech.gov.au/un-cyber-norms-resources>

In the ongoing OEWG (2021–2025), many Member States have emphasized the need to support the implementation of the Framework, including through dedicated guidance, assistance and dedicated capacity-building efforts. In response to this demand, and to increase cybersecurity and resilience of Member States, UNIDIR conducted a research study with three main objectives:

1. Identify foundational cyber capabilities (FCCs) considered necessary to effectively implement the Framework.
2. Strengthen the linkages between the Framework and States’ ability to effectively prevent or mitigate the impact of selected malicious ICT activities.

3. Design a tool to better identify requirements and prioritize capacity-building interventions, based on specific national needs and contexts, thus reinforcing the links between the implementation of the Framework and the discussions related to capacity-building, including those occurring in the current OEWG (and potential future Programme of Action).

This report focuses on objective n.1, contributes to objective n.3 and provides the basis for addressing objective n.2 which is subject of a separate publication.²

A Note on Methodology³

The research involved two phases with a mixed-methods approach. The first one focused on identifying the so-called FCCs, which are defined as the combination of policies and regulations, processes and structures, partnerships and networks, people and skills, and technology necessary to implement the Framework (see chapter 2 for definitions). This phase involved a desk-based analysis of all the agreed reports of the first OEWG (2021) and of the Groups of Governmental Experts on cyber (2010, 2013, 2015, and 2021) and additional literature. Subsequently, structured expert interviews were carried out with diplomats and cybersecurity practitioners from selected Member States and other stakeholders (including civil society and the private sector).⁴ The desk-based research and an initial set of scoping interviews were used to generate a preliminary list of FCCs. Subsequently, the second phase of the research consisted in testing the list of FCCs against specific cyber threats (ransomware, distributed denial of services (DDOS), and supply chain tampering);⁵ for this purpose, two threat-based scenarios workshops (one internal and one with external experts) were conducted.⁶ The data from these two workshops were aggregated and analysed. During a side event to the fourth session of the OEWG in New York (6–10 March 2023), UNIDIR presented the preliminary results of the research project. Finally, a final round of consultations with external experts was conducted to refine the results.

2 See Samuele Dominiononi and Giacomo Persi Paoli. 2023. Unpacking Cyber Capacity-Building: Part II. Introducing a Threat-Based Approach. UNIDIR.

3 We are grateful to the Member States and organizations that participated in the research project: Argentina, Australia, Czechia, Denmark, Estonia, Ghana, Israel, Italy, Kenya, Jamaica, Malaysia, Mauritius, Mexico, Netherlands, Singapore, and United Kingdom, and FIRST, Global Forum for Cyber Expertise, INTERPOL, International Chamber of Commerce Royal United Services Institute, Kaspersky, Microsoft, and Rajaratnam School of International Studies (RSIS).

4 The selection of the interviewees was made considering geographical and gender diversity.

5 The selection was made considering threats that are often mentioned during discussion at the multilateral level.


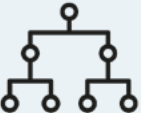
6 The external and internal expert workshops alternated plenary sessions and breakout groups to analyse, with the support of dedicated scenarios, the three case studies with a view to mapping relevant elements of the Framework to specific FCCs and related capacity-building needs. For instance, using ransomware as an entry point, participants in the workshop looked into the Framework to identify relevant norms, international law, or CBMs that could be applicable to the scenario. Then, they selected the most suitable FCCs elements to address the threat.






2. Introducing Foundational Cyber Capabilities

The FCCs are defined as the combination of policies and regulations, processes and structures, partnerships and networks, people and skills, and technology necessary to implement the Framework. For the purpose of this study, these five pillars are defined as follows.

Table 1. The Five Pillars for the Implementation of the Framework

<p>Policies and Regulations</p> 	<p>Official documents related to cybersecurity matters. These include documents outlining Member States’ positions, policies, strategies (developed specifically for key sectors, e.g. critical infrastructure, or for national-level cross-sector applications), legal and regulatory frameworks, and signatures of agreements or other forms of cooperation with international stakeholders.</p>
<p>Processes and Structures</p> 	<p>Key positions, responsible agencies/entities, other national or regional mechanisms, and official processes, procedures and protocols related to cybersecurity.</p>

<p>Partnerships and Networks</p> 	<p>Initiatives both at the domestic and international level aimed at strengthening national capacity. At the domestic level, it includes mechanisms or instruments for intrasectoral and intragovernmental cooperation. At the international level, mechanisms, or instruments for bilateral, regional, and multilateral cooperation.</p>
<p>People and Skills</p> 	<p>Knowledge and expertise related to cybersecurity. It should be noted that certain FCCs listed under the ‘people and skills’ pillar could be met also by outsourcing and establishing agreements with external providers or other stakeholders, should the State not be able to develop or sustain this specialized capability internally.</p>
<p>Technology</p> 	<p>National-level technical solutions/capabilities pertaining to cybersecurity. It should be noted that the FCCs listed under the ‘technology’ pillar could be met also by outsourcing to external service providers through, for example, public-private partnerships.</p>

It is important to note that the FCCs, developed following the methodology described in chapter 1, are intended to represent the foundational or necessary capabilities to implement the Framework. The list of FCCs is not intended to be representative of best practices or desirable measures. It has been developed with the idea of serving as a baseline upon which more refined and comprehensive responses could be developed once such a baseline is met. FCCs therefore represent minimum capability requirements necessary for the implementation of the Framework, not the optimal solutions or ideal responses. As such, elements that did not emerge as truly necessary or foundational, but more aspirational, desirable or ‘advanced’, were not included in the list.

In addition, it is also important to note that emphasis is put on what capability should be present more than on how to develop it, which remains a national prerogative. Some examples of the ‘how’ are provided in this report for illustrative purposes and to provide further guidance.

Finally, the identified FCCs serve the purpose of guiding Member States in their implementation of the Framework and they may be considered important, if not necessary, elements of the broader maturity of national cybersecurity arrangements. However, focusing on the Framework alone will not be sufficient to ensure comprehensive cyber preparedness and resilience. As such, this study complements, and is not intended to duplicate or replace, existing approaches designed with the specific purpose of assessing overall national cyber maturity or preparedness. An overview of capabilities for each component of the Framework is available in Annex 1 and further described in chapters 3-5.



3. Unpacking FCCs: Norms of Responsible State Behaviour

This section outlines the foundational cyber capabilities required for the implementation of the 11 non-binding norms of responsible State behaviour in the ICT domain (see figure 3). The chapter is structured so that each norm can be read independently, based on specific interests of the reader. As such, some FCCs may appear in multiple norms, at times as exact repetitions or with more nuanced descriptions, based on the norm. These norms were welcomed by the General Assembly of the United Nations, which in December 2015 adopted resolution 70/237. This resolution called upon Member States to be guided by 11 non-binding norms proposed by the fourth GGE. In 2021 the final report of the sixth GGE added additional information on these norms, and it reaffirmed their value for responsible State behaviour in cyberspace. The 2021 substantive report of the first OEWG also recognized and reaffirmed these 11 non-binding norms.

Figure 2. Norms of Responsible State Behaviour in Cyberspace



Source: <https://www.internationalcybertech.gov.au/un-cyber-norms-resources>

It is noteworthy to underline that there are certain norms that should be deemed essential and transversal, and therefore applicable in all scenarios and a prerequisite for the implementation of all others. This is the case for Norm A,⁷ under which general requirements underpinning inter-State cooperation are listed, as well as for Norm E⁸ that focuses on the respect and protection of human rights.

In addition to this, building on what has been affirmed in the OEWG 2021 report—“[c]apacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory”⁹—it is recommended that when Member States implement the capabilities identified in the Framework they should consider how these may affect gender dimensions differently, including gender gaps among cyber professionals,¹⁰ gender and legal responses to cyber incidents,¹¹

7 “Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.”

8 “States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.”

9 OEWG. 2021. Final Substantive Report, para. 56.

10 See Katharine Millar, James Shires, Tatiana Tropina. 2021. Gender Approaches to Cybersecurity: Design, Defence and Response. UNIDIR.

11 Ibid.

and gendered impacts of malicious ICT incidents¹² and responses.¹³ Moreover, in the current OEWG, an increasing number of States have recognized the importance of applying a gender lens to the discussions, in particular, inviting exchange on the gendered impacts of ICT incidents and narrowing the gender digital divide. Additional future research may look into providing guidance for gender mainstreaming across all the components of the framework of responsible States' behaviour.

12 See Deborah Brown and Allison Pytlak. 2020. Why Gender Matters in International Cyber Security. Women's International League for Peace and Freedom and the Association for Progressive Communications.

13 Serge Droz. 2021. Diversity and Cyber Resilience: Views of an Incident Responder. UNIDIR.

3.1 Norm A

Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

Policy and Regulations

Considering the broad spectrum of possible actions that Member States can take to implement this norm, **a national interpretation of the norm** is recommended before taking any further action. When thinking through how to implement this norm at the national level, Member States may reflect on how to cooperate with other stakeholders to achieve the objectives outlined in the norm. Subsequently, the adoption of a **cybersecurity policy, strategy, or legislation** which outlines principles and objectives (and the related implementation plan) would be key.¹⁴ In particular, it is important that the policy or strategy envisages a whole-of-government approach, which implies the possibility of taking measures at all levels of government. Moreover, Member States should define the **approach for managing cyber risk** (including for critical infrastructure) to set forth cooperation with other stakeholders.

To foster cooperative measures at the international level, public statements recognizing **cybersecurity as one of the priorities of foreign policy, a public commitment to the Framework**, and how the latter applies to the use of ICTs by States, are recommended. A public statement on **national cyber capabilities** would also contribute to increasing transparency¹⁵ and, thus, stability and peace. Finally, in light of all the skills and knowledge requirements outlined below, States are also recommended to develop **national strategies and plans for cyber skills development**.

Structures and Processes

Member States need to have or establish multiple structures to increase stability and security in the use of ICTs, including a **national centre or responsible agency or entity** (at least) that leads on cybersecurity matters; this is key to ensure coordination at the domestic level. At a more operational

14 For additional guidance on how to develop national cybersecurity strategies, refer to the Guide to Developing a National Cybersecurity Strategy produced under the coordination of the ITU with the involvement of 18 partners from international organizations, private sector, civil society and academia: <https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf>.

15 To this end Member States can make use of and inform relevant platforms (e.g., Cyber Policy Portal, Cybil, CoE Octopus platform, etc.).

level, additional key structures that Member States need to have available are **national or regional cyber-incident detection and response capabilities** (e.g., CERTs/CSIRTs or Security Operation Centres), as well as **Points of Contact (PoCs)** at the diplomatic and technical level.¹⁶ Points of contact may play a key role in enhancing communication among Member States and so contribute to de-escalating potential crises in various domains and to building confidence.¹⁷ Moreover, considering the criminal nature of many cyber incidents, **law enforcement cooperation** should be envisaged (e.g., setting up procedures on information exchange). To ensure that all the actions are taken in respect of the Framework, an **independent and effective oversight mechanism** (judiciary, administrative, parliamentary) capable of ensuring transparency, as appropriate, and accountability for State operation in the ICT domain should be established.

Partnership and Networks

As outlined in the 2021 GGE report, cooperation under this norm can be fostered at all governance levels. In light of this, two main axes of cooperation should be considered: domestic and international. On the one hand, it would be key to develop **intrasectoral** (e.g., with the private sector, civil society, and academia) and **intragovernmental cooperation** (e.g., inter-ministerial meetings, task forces) to reduce the risks of working in silos. On the other hand,

it is important to develop cooperation at the bilateral, regional, and multilateral levels on different stages (e.g., technical, law enforcement, diplomatic), and to engage with **instruments already foreseen by multilateral agreements** (e.g., the Budapest Convention for cybercrime or the Malabo convention for data protection).¹⁸

People and Skills

Given the wide range of measures that Member States can take to implement Norm A, the FCC table identifies a broad and bedrock set of skills. **Diplomatic capacities** to engage in international and intergovernmental processes dealing with ICT security are important for Member States. In light of this, diplomats would also benefit from **basic cybersecurity knowledge**. To properly engage in international forums, Member States would also need legal experts with **knowledge of international law for activities in the ICT domain**. On the other hand, considering the domestic side of the measures to increase stability and security in the use of ICT by States, it would be important to set up **‘training the trainers’** programmes on a broad portfolio of skills relating to cybersecurity (this would also contribute to limit the consequences of the global cybersecurity skills shortage). Member States should also have **cybersecurity experts and researchers** capable of keeping track of the evolving threat landscape. Finally, **systematic awareness campaigns**

¹⁶ It should be noted that, at the time of writing, the establishment of a directory of national PoCs has been extensively discussed in the context of the OEWG. A formal decision on this point is expected during the fifth official session of the OEWG planned for 24–28 July 2023. While current negotiations are focusing on a directory of PoCs at the State level, the possibility of developing an expanded directory including other stakeholders has also been proposed and discussed.

¹⁷ Samuele Dominioni. 2023. Operationalizing a Directory of Points of Contact for Cyber Confidence-Building Measures. UNIDIR.

¹⁸ This report acknowledges the ongoing negotiations of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

related to the importance of patching and other basic ‘cyber hygiene’ practices for the general public would also be relevant to the objectives of the norm.

Technology

While the norm does not imply the use of specific technologies, there are some examples of technologies that could be considered important to support the implementation of the norm. The FCCs table identifies **capabilities to ensure protection for ICT products** (such as antivirus and automatic updates/patches for digital products), **to prevent/detect/or disrupt malicious ICT acts** (such as penetration testing tools), and **to protect communication** (e.g., encryption).

3.2 Norm B

In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences.

Policy and Regulations

Attribution is a complex activity. Therefore, a founding element for the implementation of the norm is developing a **national interpretation** of it, which would cover, for example, what type(s) of attribution (technical, legal, or political)¹⁹ the State is considering and how it differentiates them. While States may decide to attribute politically based exclusively on technical attribution, it is recommended that the Member States publish **statements (or positions) concerning their interpretations of the international law** of State responsibility in the context of ICT operations. Subsequently, Member States should develop and, ideally, make publicly available, **classifications of ICT incidents in terms of scale and impact**. This would help to increase transparency around what malicious ICT incidents a Member State would interpret as an internationally wrongful act. Equally important is for Member States to develop policies outlining the **methodology and the chain of responsibility** related to the process of attribution; this would provide a useful and clear framework for decision-making related to attribution and would avoid, for example, the scenario of a Member State conducting parallel attribution processes through

different State organs without central coordination. In some cases, to carry out the attribution, Member States may need to have access to data held by non-State actors. Therefore, it is recommended to adopt **regulations establishing means to exchange information** between governmental and non-governmental stakeholders.

Structures and Processes

Given the challenges to identifying the responsible perpetrators of a malicious ICT act and to avoid the risk of misattributing it, once it has been assessed that such a malicious act violated legal or normative frameworks, Member States should attribute based on **adequate standards of proof**.²⁰ Another important element for implementing the norm relates to **processes and procedures to enable information-exchange with State and non-State actors** (including for accessing extraterritorial evidence), which may be crucial to conducting substantiated attributions.

Partnership and Networks

Malicious ICTs acts often have a cross-sectorial/national dimension. Therefore, to properly

19 See Andraz Kastelic. 2021. Non-Escalatory Attribution of International Cyber Incidents Facts, International Law and Politics. UNIDIR.

20 Although peripheral to the purpose of this study, it should be highlighted that standards of proof may also be relevant for establishing individual criminal liability and for prosecuting cybercrime more generally.

conduct attribution, cooperation between relevant domestic and international stakeholders is recommended. In terms of domestic cooperation, establishing **task forces or multi-stakeholder platforms** would serve this purpose. These would increase information-sharing and reduce the work-in-siloes effect. For what concerns international cooperation, **fostering bilateral and multilateral cooperation for assistance and information-exchange** is very important. Cooperation at the regional and international levels, including between national Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs), the ICT authorities of States and the multi-stakeholder community, can strengthen the ability of States to detect and investigate malicious ICT incidents and to substantiate their concerns and findings before reaching a conclusion on an incident. Given possible legal aspects arising from an attribution, setting up **bilateral and multilateral cooperation for the settlement of disagreement** and dispute through consultation and other peaceful means is important.

People and Skills

Conducting a substantiated attribution may involve both technical and legal skills. In terms of the first, Member States need to have available **experts to conduct technical investigation of ICT incidents** (e.g., forensic analysis for ICTs), or—in case the technical investigation is conducted by a third party—national **experts with capabilities to appraise the quality of it**. In terms of legal skills, public officers (including diplomats) should have **knowledge of legal provisions** (both at the domestic and international levels) **specific to the ICT context** and of instruments available to settle disputes on this matter peacefully or be advised on such matters by (cyber) international law advisors. In turn, in case of a dispute, public officers should be trained with **negotiation and communication skills** specific to the ICT context.

Technology

To underpin legal assessments and provide useful evidence to support political decisions regarding attribution, **technical and forensic capabilities** to investigate and determine the source of malicious ICT activity are required.

3.3 Norm C

States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

Policy and Regulations

It is recommended that Member States elaborate their **national interpretations of the norm**, including States' views on the content, scope, and conditions of the norm (e.g., what constitutes an internationally wrongful act using ICTs). Regarding norm implementation, and considering the expectation that if a State is aware of, or is notified in good faith that an internationally wrongful act using ICT is emanating from its territory, it "will take reasonable steps within its capacity to end the ongoing activity in its territory",²¹ Member States should have a **cybersecurity strategy or policy** that sets provisions to take action (e.g., detecting and interrupting) in case of a malicious ICT incident. Moreover, States should also develop appropriate legislation that defines what kind of ICT activity is and is not allowed on the territory of the State, and gives authority to investigate, end or prosecute such activities.

Structures and Processes

Appropriate structures and process are needed to enable a State to take action when it is aware, or is notified in good faith, that an international wrongful act is emanating from its territory. To this end, a **national or regional cyber-incident detection and response**

capability (e.g., a CERT/CSIRT or a Security Operation Centre) and **cyber-law-enforcement capacity** (e.g., cyber unit in the police forces) or equivalent agency with the power to investigate and prosecute, would help Member States to address threat events through means that are proportionate, appropriate and effective and in a manner consistent with international and domestic law. Moreover, considering the nature of malicious ICT incidents, it would be necessary to set up **procedures for information-sharing** among relevant domestic stakeholders (e.g., memorandums of understanding outlining cooperation between law enforcement and internet service providers). The norm also focuses on the necessity to seek assistance from other Member States. In this case, **setting up mechanisms to send or respond to requests for assistance** (including a designated national PoC/entity to receive requests for assistance and procedures for assessing the appropriateness of such requests) is relevant.

Partnership and Networks

Setting up procedures for information-sharing both domestically and internationally would require Member States to establish cooperation mechanisms. At the domestic level, it can be realized by establishing **joint task forces, multi-stakeholder platforms** (with State and

21 GGE. 2021, para. 30 (a).

non-State actors, including national CERTs/CSIRTs), and/or public-private partnerships in key sectors. At the international level, it can include bilateral or multilateral agreements for assistance and exchange of information (such as mutual legal assistance). It is also recommended to join existing frameworks for information-sharing at the technical level (e.g., the FIRST network), which bring together a wide variety of technical expertise and possibilities for cooperation across the world.

People and Skills

The norm refers to reasonable steps that the State should undertake to end malicious activity. Therefore, Member States need to

have access to **cybersecurity expertise**, either internal or external, to identify and disrupt malicious ICT acts emanating from their territory (e.g., network security skills). Another relevant set of skills concerns **communication specific to the ICT context**, including for diplomats, that would be required to manage public and confidential communication in the aftermath of an incident.

Technology

The technological capabilities related to this norm concern **identifying, detecting, and disrupting malicious ICT acts** emanating from Member States' territory.

3.4 Norm D

States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.

Policy and Regulations

This norm refers to concepts still open to interpretations (e.g., terrorist use of ICTs). Therefore, a pertinent and central capability is to publish a **national interpretation of the norm**, in which Member States elaborate their views. Additionally, it is recommended to **sign and ratify bilateral, regional or multilateral instruments** on cybercrime.²² These instruments allow for timely and effective cooperation among States. Besides, given the operational prospect of the norm, it is important that Member States adopt **policies outlining mechanisms or procedures to cooperate**, in particular, to **exchange information**, including with the private sector (e.g., through criminal procedure code). Hence, to best cooperate in these fields, it is recommended to develop **cybercrime legislation** enshrining a technology-neutral approach.²³

Structures and Processes

Establishing efficient **mechanisms to respond to and send requests for assistance** (e.g., mutual legal assistance request) is of very relevant for this norm. Equally important is to set up proper **protocols and procedures** that consent to use digital evidence in court. These protocols and procedures should set out guidelines to properly collect, handle and store digital evidence. Moreover, it is important that Member States develop and strengthen **cyber-law-enforcement capacity** (e.g., cyber police units) to be able to effectively cooperate at the operational level in contrasting criminal and terrorist use of ICTs. Additionally, a national or regional cyber incident detection and response capability (e.g., CERTs/CSIRTs or Security Operation Centres) is key to identifying, documenting, and reporting findings of malicious ICT acts.

22 While the definition of cybercrime may vary in different national legislations, for the purpose of this study we define cybercrime as offences against integrity, availability, and confidentiality of data.

23 Adopting a technology-neutral approach when drafting new bills or legal amendments on ICT allows for flexibilities in sending/receiving requests, and to keep up with the speed of technological developments; see Samuele Dominioni. 2021 Enhancing Cooperation to Address Criminal and Terrorist Use of ICTs Operationalizing Norms of Responsible State Behaviour in Cyberspace. UNIDIR.

Partnerships and Networks

The norm focuses on cooperation, which can take place at multiple levels. Member States should establish or reinforce **bilateral, regional, and multilateral mechanisms to cooperate** in investigating and prosecuting cybercrime. In this context, mutual legal assistance treaties are still prevalent. Moreover, **operational, and technical networks**, such as for law enforcement (e.g., INTERPOL I-24/7) and incident responders (e.g., FIRST), where practitioners can have quick access to relevant resources (e.g., databases) are key. Finally, **cooperation between domestic stakeholders**, including the private sector (e.g., public-private partnerships), is important to avoid working in silos and thus foster more effective and coordinated cooperation with other Member States.

People and Skills

Member States should train their personnel with different skills to properly implement the norm.²⁴ It is recommended to have **experts who can handle digital evidence at the technical and legal levels**. Training on writing

mutual legal assistance requests, using other instruments (such as the search warrant specific for digital evidence), or adequately storing and sharing data during cyber investigations is also important. Otherwise, digital evidence may not be seized or accepted in a courtroom. Member States should also have personnel with **knowledge of the legislation on cybercrime matters in other Member States**.²⁵ Finally, to improve cooperation among stakeholders, it is important that Member States' personnel (e.g., diplomats) have the **ability to connect (also informally) with bilateral, regional, and international peers** and partners to ensure efficient and timely interventions.

Technology

The technology involved in the implementation of the norm relates to two main spheres. On the one hand, there are technological capabilities to **prevent, detect, or disrupt malicious ICT acts** (e.g., threat intelligence platforms).²⁶ On the other, there are those capabilities related to **secured communication channels** or platforms for information-sharing (e.g., law enforcement software for data-sharing).

24 In this context, it is worth noting the Global Programme on Cybercrime led by UNODC: [Global Programme on Cybercrime \(unodc.org\)](https://www.unodc.org/).

25 This is important especially for Member States that need to send a request for assistance to another State; see Samuele Dominioni. 2021 Enhancing Cooperation to Address Criminal and Terrorist Use of ICTs Operationalizing Norms of Responsible State Behaviour in Cyberspace. UNIDIR.

26 A threat intelligence platform (TIP) is “a technological solution that collects, aggregates and organizes threat intel data from multiple sources and formats”; see: [https://www.paloaltonetworks.com/cyberpedia/what-is-a-threat-intelligence-platform#:~:text=A%20Threat%20Intelligence%20Platform%20\(TIP,threat%20identification%2C%20investigation%20and%20response.](https://www.paloaltonetworks.com/cyberpedia/what-is-a-threat-intelligence-platform#:~:text=A%20Threat%20Intelligence%20Platform%20(TIP,threat%20identification%2C%20investigation%20and%20response.)

3.5 Norm E

States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

Policies and Regulations

This is one of the overarching norms for all the capabilities of all the components of the framework. Therefore, to ensure its consistent implementation, Member States should publish a **national position on how International Law, including International Human Rights Law, applies to the ICT domain**. Subsequently, it is central that Member States **develop cybersecurity policies and strategies consistent with International Human Rights Law** (e.g., guidance in resolutions 68/167 and 69/166). Moreover, the norm calls for not imposing undue restrictions on freedom of expression and freedom to seek, receive and impart information. In most cases, this would be implemented by **refraining from setting up such restrictions** (e.g., censoring websites). Conversely, Member States should adopt **regulations, including for businesses, relating to the respect of human rights in the design, development, and use of new technologies**. Additionally, adopting **legislation that sets limits for State surveillance and interceptions** in line with the right to privacy is recommended. Finally, Member States should have **data protection laws** that define the legal framework on how to manage the data of natural persons.

Structures and Processes

Member States should set up **independent, effective domestic or regional oversight mechanisms** (i.e., judiciary, administrative, or parliamentary) capable of ensuring transparency, proportionality, as appropriate, and accountability for State surveillance of communications, interception, and the collection of personal data. These mechanisms can refer to specific entities (ad hoc), or to existing ones, tasked with specific authority to ensure the principles mentioned above (e.g., parliamentary committee).

Partnerships and Networks

The additional layers of understanding in the GGE 2021 report acknowledge that “a variety of stakeholders can contribute in different ways to the protection and promotion of human rights and fundamental freedoms online and offline”.²⁷ In light of this, it would be key to **engage and consult with stakeholders** who advocate, promote, and analyse (e.g., academia) human rights and fundamental freedoms online to understand and minimize the potential negative impacts of policies on people.

People and Skills

Given the overarching objective of the norm and its concrete implications, it is pertinent that public officials (including those working in law enforcement agencies) have **knowledge of human rights in the digital domain**,²⁸ as well as of **how to implement international instruments** (e.g., mutual legal assistance requests) in a way that is **consistent with human rights**. Moreover, it would be important that Member States have **experts on human rights** with expertise in their specific contexts.

Technology

There are some **technological capabilities to ensure respect for human rights** in the use of ICT technologies by States and non-State actors. Among these, endpoint cybersecurity solutions can protect from spyware, and encryption software can secure communication.

27 **GGE. 2021**, para. 41.

28 There are courses available, such as a Council of Europe course on Human Rights Education for Legal Professionals focusing on Cybercrime and E-evidence; see: [https://www.coe.int/en/web/help/courses#%2258133235%22:\[9\]](https://www.coe.int/en/web/help/courses#%2258133235%22:[9]).

3.6 Norm F

A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

Policies and Regulations

Given the focus of the norm on State obligations under international law, it is recommended that Member States develop and make publicly available their **national positions on how international law** applies to the use of ICT by States. It is important that they provide their **national interpretations** of the term “knowingly support”, their **classifications of ICT incidents** in terms of scale and seriousness (including with reference to what constitutes ‘damage’ and ‘impairment’), and their **understanding of what constitutes, considering their national context, “critical infrastructure”**.²⁹ In this way Member States can signal infrastructure or the related sectors considered critical.

Structure and Processes

To ensure that Member States abide by the objective of the norm, they should set up **independent, effective domestic or regional oversight mechanisms** (judiciary, administrative, parliamentary) capable of ensuring transparency on Member States’ conduct (e.g., parliamentary committee).

Partnerships and Networks

Given the transnational dimension of States’ conduct in the ICT domain, it would be key that Member States participate in **bilateral, regional, and multilateral framework for co-operation** to exchange information, including on their national interpretation of the norm. This could help to increase transparency around their designations and methods of categorization of critical infrastructure in order to help building common understandings regarding the protection of sectors considered critical.

People and Skills

Public officials should have **legal skills, including knowledge of international law** and its applicability in the ICT domain, to implement the norm and its relating foundational capabilities (e.g., national interpretation of the norm).

Technology

This study did not identify any foundational technological capabilities needed to implement this norm.

29 For example, healthcare, energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes, and the infrastructure essential for the general availability and integrity of the Internet; see OEWG. 2021. Final Substantive Report, para. 18.

3.7 Norm G

States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199.

Policy and Regulations

First, it would be important that Member States elaborate their **national interpretation of the norm** where they can set out their understanding of the term “appropriate”. This document should also include what are considered **the critical infrastructure sectors** to be protected, and the **classifications of ICT incidents in terms of scale and seriousness** specific to their critical infrastructure.³⁰ To protect critical infrastructure, it is key that Member States adopt a **legislative framework** suitable for this purpose (e.g., establishing regulations on their construction, including minimum security standards, reporting mechanisms, and audits). Moreover, as stated in the norm, Member States should **consider General Assembly resolution 58/199³¹** on reducing risks to critical information infrastructures in their cybersecurity policy and/or strategy. Finally, given that in many countries non-State actors play a major role in critical infrastructure management, it would be important to establish **regulations on information-exchange among the public and private sectors involved**.

Structures and Processes

In terms of structures, Member States should set up a **national centre or responsible agency for critical infrastructure** as well as **national or regional cyber-incident detection and response capabilities** (e.g., CERTs/CSIRTs or Security Operation Centres), which would play an essential role in protecting critical infrastructure. Regarding processes, it is important that Member States establish and implement **mechanisms designed to ensure compliance** with applicable standards and other regulatory requirements (e.g. auditing, testing preparedness, and scenario-based exercises to stress-test the efficacy of mechanisms/procedures for incident response), and **contingency plans** in case of ICT incidents for critical infrastructure (including measures to restore the functionality of the damaged critical infrastructure). Finally, it is necessary to implement **processes and procedures to enable information-exchange** among relevant governmental and non-governmental entities involved in the critical infrastructure ecosystem.

30 Both documents can also be issued separately.

31 This resolution, titled “Creation of a global culture of cybersecurity and the protection of critical information infrastructures”, sets out 11 elements for protecting critical information infrastructures. The resolution also invites Member States to consider these 11 elements in developing their strategies for reducing risks to critical information infrastructures, in accordance with national laws and regulations. For more information see <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/506/52/PDF/N0350652.pdf?OpenElement>.

Partnership and Networks

Given the cross-national dimension of many of the ICT incidents as well as the transnational dimension of some critical infrastructure, it is recommended that Member States set up **cross-border cooperation with relevant stakeholders** (e.g., operators, and owners) aimed at sharing information, good practice on critical infrastructure protection, and coordinating responses. This could include States' participation in voluntary risk assessment and business continuity (resilience, recovery and contingency) planning initiatives involving other stakeholders and aimed at enhancing the security and resilience of critical infrastructure that provides services regionally or internationally against existing and emerging threats. Moreover, considering the multi-stakeholder ecosystem of critical infrastructure, and to ensure a consistent and comprehensive protection, Member States should establish **cooperation mechanisms between relevant domestic stakeholders** (e.g., interagency committees, multi-stakeholder platforms), including public-private partnerships with critical infrastructure owners, operators, or managers.

People and Skills

There are several skills that Member States should take into consideration to implement this norm. First, there are **technical skills** for enhancing critical infrastructure cybersecurity protection and ICT incident response and management (e.g., network security, digital forensics, etc.). Moreover, Member States should conduct **training and exercises to test continuity of service and contingency plans** in the event of a critical infrastructure incident and encourage stakeholders to engage in similar activities. Finally, a set of skills for **diplomats to engage with their counterparts on the specific topic of critical infrastructure**, particularly if the infrastructure is transnational.

Technology

In terms of technology, it is recommended that Member States have the **technical capability to prevent, detect or disrupt malicious ICT acts targeting critical infrastructure**. These may include, but are not limited to, threat intelligence platforms,³² early warning systems,³³ tools for vulnerabilities scanning,³⁴ and secured ICT perimeters.³⁵

32 A threat intelligence platform automates the collection, aggregation, and reconciliation of external threat data; see <https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/threat-intelligence-platforms/#:~:text=A%20threat%20intelligence%20platform%20automates,risks%20relevant%20for%20their%20organization>).

33 An early warning system is a threat-notification service that informs about potentially suspicious activity on the network; see <https://www.ncsc.gov.uk/blog-post/early-warning-whats-new-and-whats-in-it-for-you>.

34 These are automated tools for discovering, analysing, and reporting on security flaws and vulnerabilities in a network.

35 For example, through the implementation of air-gapped solutions (no connection between local and external networks) or with the use of firewalls.

3.8 Norm H

States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

Policies and Regulations

The text of this norm holds several concepts and duties that Member States should clarify. Therefore, a **national interpretation of this norm** would help Member States in elucidating what they mean by, for example, “appropriate requests” or “critical infrastructure” (for this, see also Norm G). Subsequently, it is important that Member States pass legislation that provides a **framework for requesting and the delivery of international assistance and cybersecurity strategy and policies** outlining mechanisms, procedures, and processes to initiate, send, as well as respond to, requests for assistance.

Structure and Processes

Given the transnational and cooperative outlook of the norm, Member States should set up efficient **mechanisms to receive, process, evaluate and respond to, as well as to prepare and send, requests for assistance**.³⁶ Moreover, considering the enforcing

dimension of the norm, which calls for Member States to mitigate malicious ICT activity emanating from their territory, it is recommended that Member States establish **cyber-law enforcement capacities**.

Partnerships and Networks

At the international level, Member States should join **bilateral, regional, and multi-lateral cooperation instruments/agreements on protecting critical infrastructure**. These networks may help in dealing with requests for assistance (for example, they may have available common templates or specific mechanisms for crisis communication or incident management that Member States can activate). Moreover, given the role that non-State actors (often international) play in the management of critical infrastructure, it is important to set up **cross-border cooperation with relevant infrastructure owners and operators**, as well as with vendors (e.g., coordinating emergency warning systems, sharing and analysing information regarding

36 Efficient mechanisms to receive and send request for information may include the creation of templates or guiding documents about what information shall be included in the requests, establishing Points of Contact for technical matters, and an ad hoc committee or another entity to evaluate the appropriateness of a request.

vulnerabilities). Domestically, it is recommended to foster **cooperation between relevant stakeholders** in the protection of critical infrastructure (e.g., public–private partnerships, interagency committees). These provisions would help to increase information-sharing and to carry out timely and efficient interventions.

People and skills

To implement this norm, Member States should have **personnel with the ability to deal with cross-border assistance on critical infrastructure protection** (e.g., cybersecurity researchers, supply-chain risk management specialists, and incident responders). Moreover, a request for assistance may concern several aspects of critical infrastructure protection; therefore, personnel receiving or sending requests for assistance should clearly understand **how to address and manage a request for assistance**.

Technology

In terms of technology, it is important that Member States develop **capabilities to prevent, detect or disrupt malicious ICT acts targeting critical infrastructure**. These may include, but are not limited to, threat intelligence platforms,³⁷ early warning systems,³⁸ and tools for vulnerabilities scanning.³⁹ Moreover, given the focus of the norm on assistance, Member States should set up **secured communication channels or platforms** for the exchange of information pertaining to malicious ICT acts against critical infrastructure.

37 A threat intelligence platform automates the collection, aggregation, and reconciliation of external threat data; see <https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/threat-intelligence-platforms/#:~:text=A%20threat%20intelligence%20platform%20automates,risks%20relevant%20for%20their%20organization>.

38 An early warning system is a threat-notification service that informs about potentially suspicious activity on the network; see <https://www.ncsc.gov.uk/blog-post/early-warning-whats-new-and-whats-in-it-for-you>.

39 These are automated tools for discovering, analysing, and reporting on security flaws and vulnerabilities in a network.

3.9 Norm I

States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

Policies and Regulations

Considering the complexity and multi-tiered structure of contemporary supply chains, it is important that Member States define their **national interpretation of the norm** (e.g., specifying what is meant with “reasonable steps”). Moreover, it is recommended that Member States pass **legislation prohibiting the introduction of harmful hidden functions and exploitation of vulnerabilities in ICT products.**⁴⁰ This would provide the legal basis to prevent (and prosecute) malicious acts against supply chain. Additionally, it is relevant that Member States adopt a **cyber-security policy and/or strategy to address supply chain security**, possibly outlining a framework for supply-chain risk management built on a risk assessment that takes into account a variety of factors, including the benefits and risks of new technologies. Finally, to avoid the flourishing of multiple and different frameworks regulating supply-chain security, it is recommended that Member States set

out requirements to implement **globally interoperable common rules and standards for supply-chain security** (e.g., ISO/IEC 20243). Finally, considering all the security aspects involved in the production of ICT products, Member States should request vendors, to **incorporate safety and security in the ICT products’ life cycle management.**

Structure and Processes

To implement this norm, Member States should put in place **governance mechanisms for supply-chain risk management**, which includes key stakeholders representing the nodes of the value chain. This is particularly important as it would allow Member States to identify, monitor, and reviews risks to the supply chain.⁴¹ Moreover, in terms of structure, it is recommended that that Member States introduce an **assessment and certification mechanism** either by developing a dedicated national entity or by partnering with other States that already have such capability.

40 Additional examples of possible legislative interventions include measures to prevent tampering with products and services in development and production, if doing so may substantially impair the stability of cyberspace, and measures to prohibit any persons within their territory or jurisdiction to engage in cyber operations that would compromise the security, integrity or confidentiality of commercial ICT products and services.

41 To this end, Member States may mandate suppliers to use the so-called Software Bill of Materials (SBOMs—which are inventories that list all the components of software) as this would allow Member States to quickly evaluate if a supply-chain risk exists in the first place.

Finally, Member States should **ensure the interoperability** (across jurisdictions) of approaches, certification methods, and certifications of ICT products.

Partnership and Networks

Given the transnational dimensions of most supply chains, Member States should develop **cooperative measures at the bilateral, regional, and multilateral levels** to, for example, exchange good practices on supply-chain risk management or certification of ICT products, and exchange information on ICT-related vulnerabilities and/or harmful hidden functions in ICT products.

People and skills

There are different sets of skills that Member States should consider for this norm. First, there are **technical and organizational skills** to manage the security of supply chains. These include, but are not limited to, skills to identify,

monitor, and intervene to solve supply-chain vulnerabilities and assess its resilience. Subsequently, **incident responses and management skills** are also key when a malicious ICT acts occurs. Finally, given the relevance of supply chains for international security, it is relevant that Member States' **diplomats are capable of meaningfully engaging** with their counterparts on the **specific topic of supply-chain security**.

Technology

It is important that Member States are equipped with **technical capability to prevent, detect, or disrupt supply chain attacks**. These capabilities may include, but are not limited to, threat intelligence platforms,⁴² early warning systems,⁴³ and (in case Member States would like to conduct the assessment of ICT products) they should also have available tools for code sourcing and code fuzzing.⁴⁴

42 A threat intelligence platform automates the collection, aggregation, and reconciliation of external threat data; see <https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/threat-intelligence-platforms/#:~:text=A%20threat%20intelligence%20platform%20automates,risks%20relevant%20for%20their%20organization>.

43 An early warning system is a threat-notification service that informs about potentially suspicious activity on the network; see <https://www.ncsc.gov.uk/blog-post/early-warning-whats-new-and-whats-in-it-for-you>.

44 Code sourcing and code fuzzing are two methods of finding and addressing vulnerabilities in software code.

3.10 Norm J

States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

Policy and Regulations

To properly implement the norm, it is very important that Member States elaborate their **national interpretation of the norm**, which addresses, for example, how they interpret “responsible reporting” and “share associated [...] remedies”. Subsequently, from a legislative perspective, it is key that Member States adopt **legal measures to curb the commercial distribution of vulnerabilities** (for example by placing strict limits on private sector actors from developing, stockpiling, and selling ICT vulnerabilities for financial gain) and to **de-criminalize and protect cybersecurity researchers and ethical hackers** wishing to signal vulnerabilities. Equally important is to **set a coordinated vulnerability disclosure (CVD) policy** (this can be included in the cybersecurity strategy/policy or adopted as a stand-alone document) based on assumption of private disclosure over the retention of vulnerabilities.⁴⁵

Legal frameworks allowing cooperation and information-exchange with vendors

and suppliers are also recommended for sharing information on new vulnerabilities and available remedies. Regarding vendors and suppliers, it is pertinent that Member States set **precise requirements for an efficient and effective vulnerability management policy and practice** to minimize possible negative effects of vulnerable products and to systematize the reporting of ICT vulnerabilities.

Structure and Processes

Member States should establish structures and processes to make a coordinated vulnerability disclosure policy work.⁴⁶ This should include, as indicated in the GGE 2021 report, **guidance on the respective roles and responsibilities** of different stakeholders in reporting processes, the types of technical information to be disclosed or publicly shared, and handling of sensitive data to ensure the security and confidentiality of information. In addition, Member States should create **protocols for communication and information-exchange between all relevant stakeholders** (e.g., governments, suppliers/

⁴⁵ We acknowledge that certain States, in certain circumstances, may prefer not to disclose vulnerabilities. In this case, we recommend developing a vulnerability equities policy that allows Member States to assess on a case-by-case basis whether to disseminate the vulnerability information or temporarily restrict it for national security or law enforcement purposes.

⁴⁶ Good resources exist in the public domain to support States in designing their national CVD apparatus; see for example https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCVD+2022_04/about.

vendors, security researchers, and incident response teams) and for sharing updates and patching systems. Subsequently, it is important to put in place **incentives** (e.g. bug bounty programmes) and **guidance on coordinated reporting of vulnerabilities** as indicated in the GGE 2021 report (e.g. clarity on respective roles and responsibilities of different stakeholders in reporting processes, the types of technical information to be disclosed or publicly shared, and handling of sensitive data).⁴⁷ Finally, it would be key to set up **systematic awareness campaigns** (both for the general public and for the workforce of specific sectors) on the importance of patching.

Partnerships and Networks

Considering the cross-sectoral and cross-national dimensions of responsible vulnerability reporting, it is pertinent to set up specific **bilateral, regional, and multilateral cooperation** on this matter. Indeed, the GGE 2021 report mentions international cooperation as a relevant element for “a reliable and consistent process to routinize such disclosures”.⁴⁸ Equally important is to **set up cross-sectoral cooperation** with the private sector, civil society, and the technical community, including vendors and owners.

People and Skills

There are three different sets of skills that are important for the implementation of the norm. First are **technical skills**, including capacities to identify and resolve vulnerabilities and/or manage information pertaining to vulnerabilities (e.g., information provided by bug bounty companies, security researchers, and suppliers). Second, **public communication skills** are also relevant, especially when it is vital to address the general public about vulnerabilities that impact the population. Finally, in considering the possible impact of vulnerabilities on international security, **diplomatic and communication skills** are required to successfully engage in discussions about vulnerability management with relevant States and non-State actors.

Technology

There are specific **technical capabilities to identify and resolve ICT vulnerabilities** that are relevant to implement the norm. These include, but are not limited to, tools for vulnerability scanning and assessment, for vulnerability exploitability exchange (VEX),⁴⁹ and to **enforce patching at scale**, such as patch management software.

47 Governments wishing to retain the possibility of retention and non-disclosure should develop a dedicated process, outlined in a public-facing document, to manage when and how a government will choose to disclose cyber vulnerabilities it either uncovers or purchases. This process should include, for example, an inter-agency vulnerability review committee, clear criteria used for determining whether to disclose a vulnerability, and the mechanism for handling disagreements within the committee. See for example <https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>

48 GGE. 2021, para. 61.

49 “Vulnerability exploitability exchange (VEX) is a system for software producers to share with software consumers an assessment on the vulnerabilities present in their software components. VEX is the mechanism through which software producers classify and label the vulnerabilities in their software. [...] They also include an analysis of the vulnerabilities such as if the vulnerability may or may not be exploitable and why, and how the vulnerability can be mitigated or fixed, and any known workarounds that can be used to protect against it”; see <https://www.endorlabs.com/blog/what-is-vex-and-why-should-i-care>.

3.11 Norm K

States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Policies and Regulations

To properly implement the norm, Member States should outline their **position on the norm** or on certain aspects of it. For example, it would be key to define the national position on the applicability of international law on the use of ICT by States, on the concepts of “malicious international activity” and “knowingly support”. To signal to the international community that a Member State is committed to respecting the norm, it is recommended that it publishes a **statement declaring it will not use authorized emergency response teams to engage in malicious or offensive international activity**. Equally important, as a signal to other States, is for Member States to issue a **list of all declared CSIRT/CERTs on their territory**. Domestically, Member States should outline in their cybersecurity policy and/or strategy **clear status, authority, and mandates of their CERTs/CSIRTs** (which distinguish their unique and neutral functions from other government functions). Finally, given the neutral and unique function of these cyber-incident detection and response teams, it is important to set a **regulatory framework for the work of CERTs/CSIRTs in line with international guidelines and standards** (e.g., FIRST code of ethics or ISO 27/2001).

Structures and processes

Although the norm does not require Member States to establish national (or regional) cyber-incident response capabilities, as it is indicated among the capabilities under Norm A, it is recommended that Member States **set up a national CSIRT/CERT or join a regional one**. Moreover, considering the intent of the norm, it is important that Member States **establish independent and effective oversight mechanisms** (judiciary, administrative, parliamentary) capable of ensuring transparency, as appropriate, and accountability for State operation in the ICT domain (e.g., parliamentary committee).

Partnerships and Networks

This study did not identify any foundational capabilities concerning partnerships and networks needed to implement this norm.

People and Skills

It is very important that Member States can identify and document possible cases of misuse of CSIRT/CERTs engaged in malicious activities. Therefore, Member States should have available **experts to conduct technical**

investigations of these activities (e.g., forensic analysts for ICTs) or—in case the technical investigation is conducted by a third party—to appraise the quality of it. Moreover, it is important that there is **awareness among public officials** (including armed forces) about the role and status of CERTs/CSIRTs. Finally, **legal expertise, including in international law specific to the ICT domain**, is key to properly implementing several elements (e.g., to draft

the national interpretation of the norm) pertaining to the implementation of the norm.

Technology

This study did not identify any foundational technological capabilities needed to implement this norm.



4. International Law

In the previous chapter, specific elements of international law have been flagged in relation to specific norms. This section provides a more general overview of the FCCs concerning international law that go beyond the norm-specific requirements outlined previously. The substantive report of the OEWG 2019-2021 underlines that, “[r]ecognizing General Assembly Resolution 70/237, and also acknowledging General Assembly resolution 73/27, which established the OEWG, States reaffirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT”.⁵⁰

Policies and Regulations

Member States agreed that international law applies to ICT and that “further common understandings need to be developed on how international law applies to State use of ICTs”.⁵¹ To promote the development of a common understanding of how international law applies, it is recommend that Member States elaborate and exchange their views on this matter. As such, as a starting point, States should **develop public-facing national positions on the applicability of international law to the ICT context.**

50 [OEWG, 2021. Final Substantive report](#), para. 34.

51 *Ibid.*

Structure and Processes

To ensure that Member States' behaviour in cyber space and use of ICTs is lawful, and to hold them accountable, it is recommended that Member States establish (at the national or regional level) an **independent oversight mechanism** (judiciary, administrative, parliamentary).

Partnerships and Networks

Given the current challenges concerning developing a common understanding of how international law applies to the use of ICT, it is important that Member States put forward **co-operation mechanisms** (e.g., sharing lessons learned, setting up visiting programmes for legal experts, exchanging information) in the areas of international law, national legislation, and policies. Moreover, it is recommended that Member States **actively participate in multi-lateral processes dealing with international law in the ICT domain** (e.g., the OEWG).

People and Skills

Applying international law in the ICT domain or developing a national view on the matter, requires States to develop or secure **access to specialized legal expertise**. Subsequently, it is also key for a Member State to be able to engage in **international law discussions at the regional and international levels** (including the capacity to engage with the broader academic and civil society community). In these settings, it is recommended that legal experts/practitioners be able to meaningfully engage in activities in a language that may be different from their own mother tongue.

Technology

This study did not identify any foundational technological capabilities needed to implement this norm.



5. Confidence-Building Measures

Similarly to international law, norm-specific confidence-building measures have already been listed where appropriate in the various sections of Chapter 3. This chapter provides a more general overview of additional confidence-building measures that States should consider implementing at the national level. As affirmed in the substantive report of the first OEWG, “[c]onfidence-building measures (CBMs), which comprise transparency, cooperative and stability measures can contribute to preventing conflicts, avoiding misperception and misunderstandings, and the reduction of tensions. They are a concrete expression

of international cooperation”.⁵² Hereunder the report outlines the FCC concerning the CBMs.

Policies and Regulations

In terms of policies and regulations to foster transparency, it is recommended that Member States **publicly release all relevant national cybersecurity strategies, policies, and regulations**, ideally with an official translation in English (at least) to facilitate access. Moreover, it is important that Member States **identify and consider CBMs appropriate to their specific context** and adopt policies and

52 OEWG. 2021. [Final Substantive report](#), para. 41.

regulations to cooperate with other States on their implementation (e.g., adopting templates for information-sharing or establishing points of contact at the national level).

Structures and Processes

One of the essential elements of confidence-building is the **establishment of a point of contact**. Establishing PoCs at the technical and diplomatic level is important to ensure direct communication between Member States; this is key not only in relation to the implementation of specific norms, but especially in times of crisis. Additionally, to foster transparency, cooperation, and stability, Member States should set up **national or regional cyber-incident response capabilities** (e.g., CERTs/CSIRTs). Due to their role as ‘first responders’ these structures play a relevant role in addressing incidents or threats as soon as they occur. In doing so, they often interact with their counterparts abroad. In turn, their interactions contribute to increasing transparency and cooperation. In terms of processes, it is very important that Member States **share information and good practices on several related topics**, including existing and emerging ICT threats and incidents, standards for vulnerability analysis of ICT products, as well as exchange information on national approaches to ICT security and data protection. In doing so, Member States can use the Cyber Policy Portal of the United Nations Institute for Disarmament Research.⁵³

Partnerships and Networks

Confidence-building measures are possible as long as Member States get involved with others in international settings. Therefore, it

is recommended that Member States **participate in United Nations processes** (such as the OEWG, which has been recognized as a confidence-building measure itself), become involved in **dialogue through bilateral, sub-regional, regional, and multilateral consultations**, and that they engage with **regional bodies that developed and implemented CBMs**. Additionally, it is very important that Member States **participate in frameworks for cooperation among CERTs/CSIRTs** (or other technical security bodies), such as the FIRST network or other regional frameworks. These frameworks offer a unique opportunity to develop relationships that increase trust among the technical community.

People and Skills

Member States should retain experts with **knowledge of existing CBMs** and how to activate or leverage them in time of crisis. In particular, given the key role of PoCs, having **staff prepared to effectively act as PoC** is recommended (e.g., conducting training in PoC function and processes). Moreover, it is important that Member States have personnel capable of **making use of information-sharing platforms** (e.g., the UNIDIR Cyber Policy Portal), which are considered important tools to foster transparency. Finally, confidence building requires **communication and diplomatic skills** for public officials to engage in cybersecurity discussions with their counterparts.

Technology

Trusted channels and platforms for communication among States are important for confidence-building engagements.

53 <https://cyberpolicyportal.org/>.



6. Conclusions

With the continuously evolving cyber threat landscape, it is important that States maximize their ability to prevent, or mitigate the consequences of, malicious ICT acts. As part of this effort, being able to implement the Framework for Responsible State Behaviour in cyberspace is an important step to increase national cyber resilience and a necessary one to ensure peace and security in the ICT domain.

The foundational cyber capabilities identified in this report are intended to represent a baseline from which more elaborate or advanced measures can be developed. Nevertheless, the list of capabilities identified shall not be considered closed or definitive. Given the continuous and rapid developments in the ICT domain (e.g., in the case of widespread adoption of new disruptive technologies like artificial intelligence or quantum computing), additional elements may become relevant and foundational for existing norms or as new norms are developed.

It should be noted that, while the purpose of this study is not to rank or assign specific ‘weights’ to individual FCCs or norms, an analysis of the overall FCCs distribution suggests that five key elements emerge as particularly prominent:

- a. a comprehensive national cybersecurity strategy/policy;
- b. a dedicated entity to act as focal point/national coordinator on cyber matters;
- c. an emergency or incident response capability (national or regional);

- d. well-structured cooperation with all relevant stakeholders, including private sector and critical infrastructure operators; and
- e. access to specialized skills (e.g. technical, legal, diplomatic, communications).

These five key elements are among the most recurrent capabilities relevant for almost all the components of the Framework. Therefore, by setting these elements up, Member States may be advantaged in the implementation of the entire Framework. Moreover, as mentioned in chapter 2, it is very important that Member States when implementing the foundational cyber capabilities do so in full respect of human rights and in consideration of the gender dimensions. Future research endeavours may unpack each FCC pillar, or element, to deepen the understanding of the gender dynamics involved and better frame their formulation and implementation.

The FCCs presented in this report constitute the elements through which Member States can implement the Framework and foster international peace, security, cooperation, and trust in the ICT environment. The second part of this study, titled “Introducing a Threat-Based Approach”, proposes an approach that would allow governments to better assess their readiness to leverage the Framework to prevent or respond to specific malicious ICT activities and threats.



Annex 1. Foundational Cyber Capabilities Table



Norm A

States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

POLICY AND REGULATION

i	National interpretation of the norm.
ii	Cybersecurity policy and strategy (and national implementation plan), or law/legislation on national cybersecurity (preferably outlining a whole-of-government approach).
iii	Cyber risk management approach (including for critical infrastructure).
iv	Foreign policy that recognizes cybersecurity as one of the priorities.
v	Public commitment to the Framework for Responsible State Behaviour in cyberspace.
vi	Public statement on national cyber capabilities available (not classified information).
vii	National strategies and plans for cyber skills development.

STRUCTURE AND PROCESSES

i	National centre or responsible agency/entity for cybersecurity.
ii	National, or regional, cyber-incident detection and response capabilities (e.g., CERTs/CSIRTs or Security Operation Centre).
iii	Point of Contact (PoC) at the diplomatic and technical level.
iv	Law and enforcement cooperation and information-exchange.
v	Independent and effective oversight mechanisms (judiciary, administrative, parliamentary) capable of ensuring transparency, as appropriate, and accountability for State operation in the ICT domain.

PARTNERSHIPS AND NETWORKS

i	Intrasectoral cooperation (private sector, civil society, technical community, academia).
ii	Intragovernmental cooperation (e.g., interministerial meetings, task forces).
iii	Bilateral, regional, and multilateral cooperation at different levels (technical, operational, diplomatic).
iv	Multilateral agreements (e.g., the Budapest Convention, the Malabo Convention).

PEOPLE AND SKILLS

i	Diplomatic capacities to engage in international and intergovernmental processes.
ii	Basic cybersecurity knowledge for policy experts and practitioners.
iii	Legal skills for legal experts on international law for activities in the ICT domain.
iv	“Training the trainer” programmes and professional certification.
v	Skills to manage cybersecurity incidents, including readiness, response, and recovery, both at the domestic and international levels.
vi	Systematic awareness campaigns for the general public related to the importance of patching and other basic cyber hygiene practices, such as software updates.

TECHNOLOGY

i	Capabilities to ensure cybersecurity endpoint protection (antivirus or automatic updates/patches for digital products to mitigate security bugs and vulnerabilities.).
ii	Technical capability to prevent, detect or disrupt malicious ICT acts.
iii	Technical solutions to protect communications (e.g., encryption).

2

CONSIDER
ALL RELEVANT
INFORMATION

Norm B

In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

POLICY AND REGULATION

i	National interpretation of the norm.
ii	National position(s), or statement(s), on the application of international law to the use of ICTs by States.
iii	Classification (public or non-public) of ICT incidents in terms of scale and impact.
iv	Policy (public or non-public) on attribution including definitions, methodology, and clear roles and responsibilities.
v	Regulation allowing the exchange of information with relevant commercial and other non-governmental entities.

STRUCTURE AND PROCESSES

i	National standards of proof for attribution.
ii	Process and procedures to enable information-exchange among relevant governmental and non-governmental entities.

PARTNERSHIPS AND NETWORKS

i	Cooperation between relevant domestic stakeholders (e.g., task forces, multi-stakeholder platforms).
ii	Bilateral and multilateral cooperation for assistance and exchange of information at the international level.
iii	Bilateral and multilateral cooperation for the settlement of disagreements and disputes through consultation and other peaceful means.

PEOPLE AND SKILLS

i	Skills to conduct (or appraise, if the information is provided by third parties) technical investigations of ICT incidents.
ii	Legal skills for public officers (including diplomats) specific to the ICT context, including on consultation and other peaceful means to settle disputes at the international level.
iii	Negotiation and communication skills for public officers (including diplomats) specific to the ICT context.

TECHNOLOGY

i	Technical and forensic capabilities to investigate and determine the source of malicious ICT activity.
---	--

3 PREVENT MISUSE OF ICTs IN YOUR TERRITORY



Norm C

States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs

POLICY AND REGULATION

- i National interpretation of the norm (including the State's view on internationally wrongful acts using ICTs).
- ii Cybersecurity strategy and policy including provisions to prevent, detect, and interrupt the malicious use of ICTs.
- iii Specific legislation that defines what ICT activities are not allowed on the territory, and that it gives authority to investigate, end or prosecute such activities.

STRUCTURE AND PROCESSES

- i National, or regional, cyber-incident detection and response capabilities (e.g., CERTs/CSIRTs or Security Operation Centre).
- ii Cyber-law-enforcement capacity.
- iii Procedure for information-sharing among relevant domestic stakeholders, including non-governmental entities.
- iv Mechanisms to send or respond to requests for assistance (including procedures for assessing such requests).

PARTNERSHIPS AND NETWORKS

- i Cooperation between relevant domestic stakeholders (e.g., task forces, multi-stakeholder platforms), including relevant public-private partnerships.
- ii Bilateral and multilateral agreement for assistance and exchange of information.
- iii Framework for information-sharing at the technical level (such as the FIRST network).

PEOPLE AND SKILLS

- i Ability to identify and disrupt malicious ICT acts emanating from own territory.
- ii Communication skills for public officers (including diplomats) specific to the ICT context.

TECHNOLOGY

- i Technical capability to prevent, detect or disrupt malicious ICT acts emanating from own territory.

4 COOPERATE TO STOP CRIME & TERRORISM



Norm D

States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats.

POLICY AND REGULATION

i	National interpretation of the norm.
ii	Signature and ratification of bilateral, regional, or multilateral instruments on cybercrime.
iii	Policies outlining mechanisms or procedures to cooperate and exchange information, including with relevant commercial and other non-governmental entities.
iv	Cybercrime legislation enshrining a technology-neutral approach.

STRUCTURE AND PROCESSES

i	Mechanism to respond to and send requests for assistance (such as for mutual legal assistance requests).
ii	Protocols and procedures for collecting, handling, and storing digital evidence.
iii	Cyber-law-enforcement capacity.
iv	National, or regional, cyber-incident detection and response capabilities (e.g., CERTs/CSIRTs or Security Operation Centre).

PARTNERSHIPS AND NETWORKS

i	Bilateral, regional, and multilateral cooperation for investigation, assistance, law enforcement, and exchange of information concerning criminal and terrorist use of ICTs (e.g., mutual legal assistance treaties).
ii	Operational (e.g., INTERPOL I-24/7) and technical networks (e.g., FIRST).
iii	Cooperation between relevant domestic stakeholders (e.g., task forces, multi-stakeholder platforms), including through structured public-private partnerships.

PEOPLE AND SKILLS

i	Ability to handle digital evidence at the technical and legal levels.
ii	Knowledge of the legislation on crime and terrorism in other Member States.
iii	Ability to connect with bilateral, regional, and international peers and partners to ensure efficient and timely interventions.

TECHNOLOGY

i	Technical capability to prevent, detect or disrupt malicious ICT acts conducted by criminals and terrorists.
ii	Secured communication channels or platforms for information-sharing.

5 RESPECT HUMAN RIGHTS & PRIVACY



Norm E

States, in ensuring the secure use of ICTs, should guarantee full respect for human rights, including the right to freedom of expression.

POLICY AND REGULATION

i	National position on the applicability of international law, including international human rights law.
ii	Cybersecurity policy and strategy consistent with international human rights law (e.g., guidance in resolutions 68/167 and 69/166).
iii	No undue restrictions on freedom of expression and freedom to seek, receive and impart information.
iv	Regulations for the design, development, and use of new technologies (including for businesses) respectful of human rights.
v	Legislation on State surveillance and interceptions in line with the right to privacy.
vi	Data protection law.

STRUCTURE AND PROCESSES

i	Independent, effective domestic or regional oversight mechanisms (judiciary, administrative, parliamentary) capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception, and the collection of personal data.
---	---

PARTNERSHIPS AND NETWORKS

i	Engagement and consultation with stakeholders who advocate, promote, and analyse human rights and fundamental freedoms online to understand and minimize potential negative impacts of policies on people.
---	--

PEOPLE AND SKILLS

i	Knowledge among public officials (including law enforcement agencies) of human rights in the digital domain, as well as of how to implement international instruments in a way that is consistent with human rights.
ii	Localized/contextualized expertise, including legal, on human rights.

TECHNOLOGY

i	Technical capability to ensure respect of human rights in the use of ICT technologies by States and non-State actors
---	--

**6 DO NOT DAMAGE
CRITICAL
INFRASTRUCTURE**



Norm F

A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages or impairs critical infrastructure.

POLICY AND REGULATION

- i** National position on the applicability of international law, including on the use of ICT by States.
- ii** National interpretation of the norm.
- iii** Classification (public or non-public) of ICT incidents in terms of scale and seriousness.
- iv** National understanding of critical infrastructure.

STRUCTURE AND PROCESSES

- i** Independent, effective domestic or regional oversight mechanisms (judiciary, administrative, parliamentary) capable of ensuring transparency, as appropriate.

PARTNERSHIPS AND NETWORKS

- i** Bilateral, regional, and multilateral frameworks for cooperation and exchange of information.

PEOPLE AND SKILLS

- i** International law expertise specific to activities conducted in the ICT domain.

TECHNOLOGY

N/A

7

PROTECT
CRITICAL
INFRASTRUCTURE

Norm G

States should take appropriate measures to protect their critical infrastructure from ICT threats.

POLICY AND REGULATION

i	National interpretation of the norm.
ii	National designation of critical infrastructure sectors.
iii	Classification (public or non-public) of ICT incidents in terms of scale and seriousness.
iv	Legislation on the protection of critical infrastructure (establishing regulations, reporting, audits, etc.).
v	Cybersecurity strategy and policy including provisions on cyber risk reduction for critical infrastructure, cybersecurity measures for ICT products and taking into account resolution 58/199 on the global culture of cybersecurity and critical information infrastructure protection.
vi	Regulation allowing the exchange of information with relevant commercial and other non-governmental entities.

STRUCTURE AND PROCESSES

i	National centre(s) or responsible agency(ies) for critical infrastructure.
ii	National, or regional, cyber-incident detection and response capabilities (e.g., CERTs/CSIRTs or Security Operation Centre).
iii	Cybersecurity compliance mechanisms for critical infrastructure.
iv	Contingency plans in case of ICT incidents concerning critical infrastructure.
v	Process and procedures to enable information-exchange among relevant governmental and non-governmental entities.

PARTNERSHIPS AND NETWORKS

i	Cross-border cooperation with relevant infrastructure owners and operators (e.g., coordinating responses to incidents, sharing good practices on critical infrastructure protection).
ii	Cooperation between relevant domestic stakeholders (e.g., inter-agency committee, multi-stakeholder platforms), including public-private partnerships with critical infrastructure owners, operators, or managers.

PEOPLE AND SKILLS

i	Technical skills required to protect national critical infrastructure from malicious ICT acts.
ii	Training and exercises to enhance response capabilities and to test continuity and contingency plans in the event of a critical infrastructure attack and encourage stakeholders to engage in similar activities.
iii	Ability of diplomats to meaningfully engage with their counterparts on the specific topic of critical infrastructure, particularly if the infrastructure is transnational.

TECHNOLOGY

i	Technical capability to prevent, detect or disrupt malicious ICT acts targeting critical infrastructure.
---	--

8**RESPOND TO REQUESTS FOR ASSISTANCE****Norm H**

States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts.

POLICY AND REGULATION

- i** National interpretation of the norm.
- ii** Legislation providing a framework for requesting and delivering international assistance.
- iii** Cybersecurity strategy and policies outlining mechanisms/procedures/processes to respond to requests for assistance.

STRUCTURE AND PROCESSES

- i** Efficient mechanisms to receive, process, evaluate and respond to requests for assistance as well as to prepare and send requests for assistance.
- ii** Cyber-law-enforcement capacity.

PARTNERSHIPS AND NETWORKS

- i** Bilateral, regional and multilateral cooperation on critical infrastructure protection (e.g., creating common templates for requesting assistance, signing Memorandums of Understanding, etc.).
- ii** Cross-border cooperation with relevant infrastructure owners and operators, as well as with vendors (e.g., coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities).
- iii** Cooperation between relevant domestic stakeholders (e.g., public-private partnership, inter-agency committees).

PEOPLE AND SKILLS

- i** Ability to provide effective and timely cross-border assistance to States targeted by attacks against critical infrastructure.
- ii** Skills to address and manage requests for assistance.

TECHNOLOGY

- i** Technical capability to prevent, detect or disrupt malicious ICT acts targeting critical infrastructure.
- ii** Secured communication channels or platforms for the exchange of information pertaining to malicious ICT acts against critical infrastructure.

9**ENSURE SUPPLY
CHAIN SECURITY****Norm I**

States should take reasonable steps to ensure the integrity of the supply chain and should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

POLICY AND REGULATION

- | | |
|------------|--|
| i | National interpretation of the norm. |
| ii | Laws and regulations prohibiting the introduction of harmful hidden functions and exploitation of vulnerabilities in ICT products. |
| iii | Cybersecurity policy and strategy addressing supply-chain security and outlining milestones. |
| iv | Requirement to implement globally interoperable common rules and standards for supply-chain security (e.g., ISO/IEC 20243). |
| v | Requirement for vendors to incorporate safety and security in ICT product life cycle management. |

STRUCTURE AND PROCESSES

- | | |
|------------|--|
| i | Supply-chain risk-management governance mechanism (with key stakeholders representing every node of the value chain). |
| ii | Assessment and certification mechanism for ICT products (domestic or in partnership with other countries). |
| iii | Agreements to ensure the interoperability across jurisdictions of approaches, certification methods, and certifications of ICT products. |

PARTNERSHIPS AND NETWORKS

- | | |
|----------|--|
| i | Cooperative measures (e.g., exchange of good practices on supply-chain risk management, certification of ICT products) at the bilateral, regional, and multi-lateral levels. |
|----------|--|

PEOPLE AND SKILLS

- | | |
|------------|--|
| i | Supply-chain security and supply-chain risk-management skills. |
| ii | Incident response and management skills. |
| iii | Ability of diplomats to meaningfully engage with their counterparts on the specific topic of supply-chain security and supply-chain attacks. |

TECHNOLOGY

- | | |
|----------|--|
| i | Technical capability to prevent, detect or disrupt supply-chain attacks. |
|----------|--|



Norm J

States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT dependent infrastructure.

POLICY AND REGULATION

i	National interpretation of the norm.
ii	Legal measures to curb the commercial distribution of vulnerabilities.
iii	Decriminalization and legal protection for security researchers and ethical hackers wishing to signal vulnerabilities.
iv	Coordinated vulnerability disclosure (CVD) policy.
v	Legal frameworks to allow cooperation and information-exchange with vendors and suppliers.
vi	Requirements for efficient and effective vulnerability management policy and practice.

STRUCTURE AND PROCESSES

i	Guidance on the respective roles and responsibilities of different stakeholders in reporting vulnerabilities (including the types of technical information to be disclosed, how to handle sensitive data, etc.).
ii	Established protocols for communication and information-exchange between all relevant stakeholders (e.g., governments, suppliers/vendors, security researchers, incident response teams).
iii	Established protocols for updating and patching systems, particularly those pertaining to ICT-dependent infrastructure.
iv	Guidance and incentives on coordinated reporting of vulnerabilities (e.g., bug bounty programme).
v	Systematic awareness campaigns (both for the general public and targeted to employees of specific industries, particularly those operating in the critical infrastructure sectors) related to the importance of patching.

PARTNERSHIPS AND NETWORKS

i	Bilateral, regional, and multilateral cooperation for vulnerability disclosures.
ii	Cross-sectoral cooperation (private sector, civil society, technical community, including vendors and owners).

PEOPLE AND SKILLS

i	Technical skills required to identify and resolve vulnerabilities and/or to manage information pertaining to vulnerabilities once received from third parties (e.g., bug bounty companies, security researchers, suppliers).
ii	Public communication skills required to address vulnerabilities, particularly when they have impact on the general population.
iii	Diplomatic and communication skills required to successfully engage in discussions about vulnerability management with relevant State and non-State actors.

TECHNOLOGY

i	Technical capability to identify and resolve ICT vulnerabilities or to take action when information is provided by third parties.
ii	Technical capability to enforce patching at scale.



Norm K

States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

POLICY AND REGULATION

i	National position on the norm (or certain aspects of it).
ii	Public statement that the State will not use authorized emergency response teams to engage in malicious or offensive international activity (and respect the ethical principles that guide the work of these bodies).
iii	List of all declared CERTs/CSIRTs.
iv	Cybersecurity policy and/or strategy with clear status (such as critical infrastructure), authority, and mandates of CERTs/CSIRTs (which distinguish their unique and neutral functions from other government functions).
v	Regulatory framework for the work of CERTs/CSIRTs in line with international guidelines and standards (e.g., FIRST code of ethics, or ISO 27/2001).

STRUCTURE AND PROCESSES

i	National (or regional) cyber-incident response capabilities (e.g., CERTs/CSIRTs or Security Operation Centre).
ii	Independent and effective oversight mechanisms (judiciary, administrative, parliamentary) capable of ensuring transparency, as appropriate, and accountability for State operation in the ICT domain.

PARTNERSHIPS AND NETWORKS

N/A

PEOPLE AND SKILLS

i	Skills to conduct (or appraise, if the information is provided by third parties) technical investigations of misuse of CERTs and CSIRTs to conduct malicious activity.
ii	Awareness among public officials (including armed forces) about the role and status of CERTs/CSIRTs.
iii	Legal expertise, including on international law, specific to the ICT domain.

TECHNOLOGY

N/A



International Law

Note: this section of the FCC table includes additional international law elements that should be considered as complimentary/supplementary to the specific ones included under each norm.

POLICY AND REGULATION

- i Public statement of State's understanding of how international law applies to cyberspace.

STRUCTURE AND PROCESSES

- i Independent oversight mechanisms (judiciary, administrative, parliamentary) to ensure the lawfulness and accountability of State operations in the ICT domain.

PARTNERSHIPS AND NETWORKS

- i Cooperation with other Member States in the areas of international law, national legislation, and policies.
- ii Active participation in multilateral processes dealing with international law in the ICT domain.

PEOPLE AND SKILLS

- i Legal expertise in international law, and States' responsibilities in the cyber domain.
- ii Ability to engage in international law discussions at the regional and international levels (including capacity to engage with the wider academic and civil society community), in a language that may be different from their own mother tongue.

TECHNOLOGY

N/A



Confidence-Building Measures

POLICY AND REGULATION

- | | |
|----|---|
| i | Publicly release all relevant national cybersecurity strategies, policies, and regulations, ideally with an official translation (at least) in English to facilitate access and transparency. |
| ii | Identify and consider CBMs appropriate to their specific context and cooperate with other States on their implementation. |

STRUCTURE AND PROCESSES

- | | |
|-----|--|
| i | Establishment of national Point(s) of Contact (PoCs) at the diplomatic and technical levels. |
| ii | National, or regional, cyber-incident response capabilities (e.g. CERTs/CSIRTs or Security Operation Centre). |
| iii | Share information and good practices, lessons, or white papers: <ul style="list-style-type: none"> on existing and emerging ICT security-related threats and incidents; national strategies and standards for vulnerability analysis of ICT products; national and regional approaches to risk management and conflict prevention. |
| iv | Exchange information on: <ul style="list-style-type: none"> national approaches to ICT security; data protection; the protection of ICT-enabled critical infrastructure; ICT-security agency mission and functions, and ICT strategy at the national or organizational levels, and the legal and oversight regimes under which they operate. |

PARTNERSHIPS AND NETWORKS

- | | |
|-----|---|
| i | Participation in United Nations processes (such as the OEWG). |
| ii | Engage in dialogue through bilateral, sub-regional, regional and multilateral consultations. |
| iii | Engage in/with regional bodies that develop and implement CBMs. |
| iv | Participate in frameworks of cooperation among CERTs/CSIRTs (or other technical security bodies), such as the FIRST network or other regional frameworks. |

PEOPLE AND SKILLS

- | | |
|-----|---|
| i | Knowledge of existing CBMs and ways to activate/leverage them in time of crisis. |
| ii | Knowledge and competencies required to effectively act as national PoC (if nominated). |
| iii | Ability to make use of existing information-sharing platforms (e.g., UNIDIR's Cyber Policy Portal). |
| iv | Diplomatic and communication skills required to effectively engage in cybersecurity discussions with counterparts in other countries. |

TECHNOLOGY

- | | |
|---|--|
| i | Trusted channels and platforms for communication among States. |
|---|--|

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



UNIDIR

Palais de Nations
1211 Geneva, Switzerland

© UNIDIR, 2023

WWW.UNIDIR.ORG