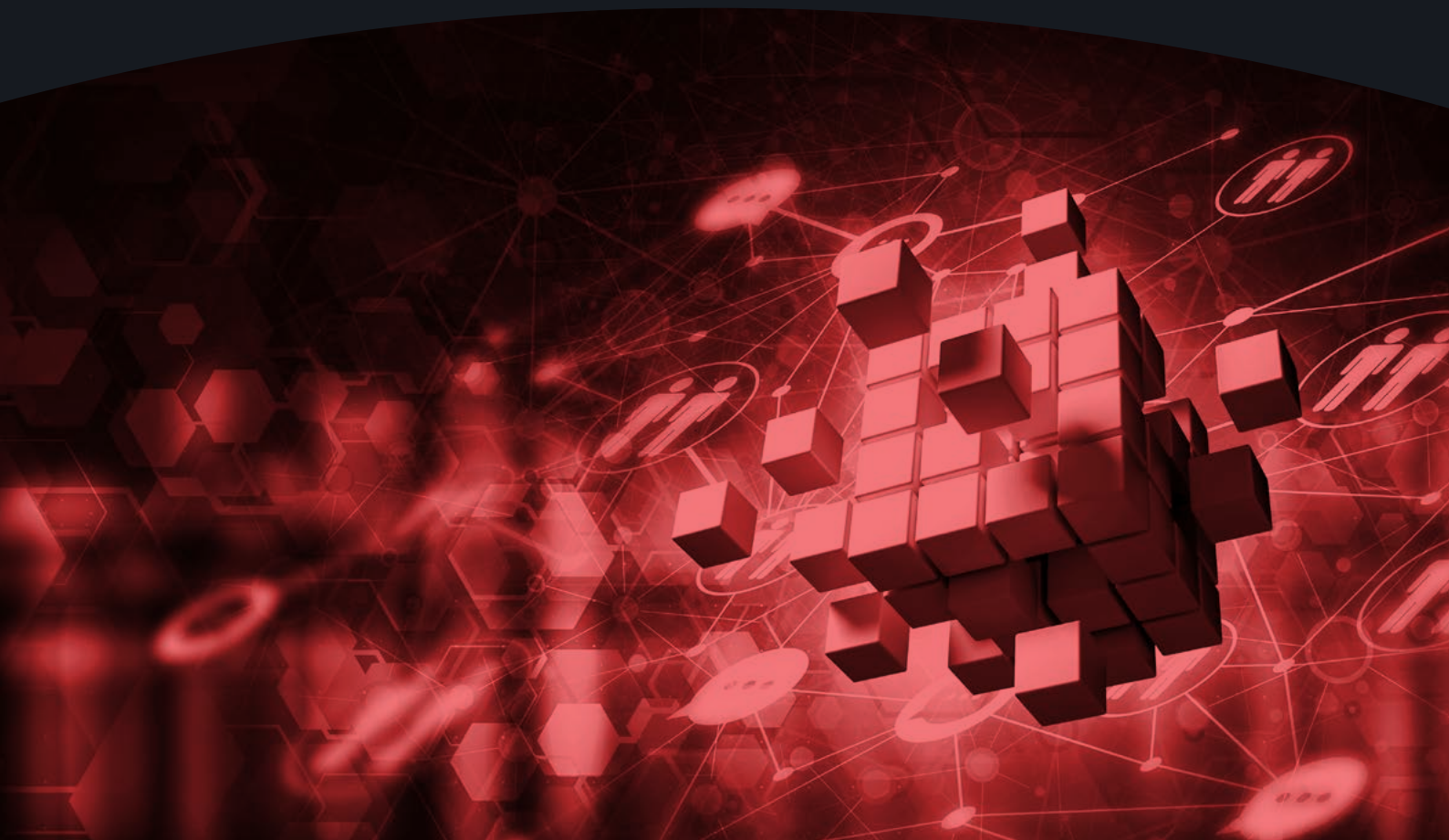
UNIDIR

Unpacking Cyber Capacity-Building Needs

Part II. Introducing a Threat-Based Approach

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

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

Acronyms & Abbreviations

CBM	Confidence-Building measures
CERT/CSIRT	Computer Emergency Response Team/Computer Security Incident Response Team
DDOS	Distributed Denial of Service
FCC	Foundational Cyber Capabilities
GGE	Group of Governmental Experts
ICT	Information Communication Technologies
IL	International Law
OEWG	Open Ended Working Group
UNIDIR	United Nations Institute for Disarmament Research
UNODA	United Nations Office for Disarmament Affairs

Executive Summary

As States continue to discuss the four key pillars of the Framework for Responsible State Behaviour in the use of ICTs (henceforth, the Framework)—norms of responsible behaviour, international law, confidence-building measures and capacity-building—two key aspects remain under-explored:

a. the extent to which the implementation of the Framework can be used to increase national, regional and international security and resilience against specific threats; and
b. how specific threats can be used to inform capacity-building initiatives.

The threat landscape in the ICT domain is constantly evolving, becoming more complex and sophisticated as cybersecurity measures continue to improve. While it should be noted that more than 90 per cent of cyberattacks could be prevented by the systematic application of basic security 'hygiene', the Framework can provide an important additional layer of resilience. Indeed, putting in place the capabilities necessary to implement the Framework would equip States with important tools that can contribute to the prevention or mitigation of specific cyber threats as well as to the strengthening of their overall cyber resilience.

This report is the second of a two-part study conducted by UNIDIR and aims at strengthening the linkages between the Framework and States' abilities to effectively prevent or mitigate the impact of selected malicious ICT activities. The report is centered on the concept of Foundational Cyber

Capabilities (FCCs), introduced in the first part of the study, 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.

This report 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. The proposed 'threat-based approach' encompasses three steps.

- **Step 1. Threat and risk assessment:** in this step, a given government should map, assess and prioritize ICT threats that are affecting its territory.
- **Step 2. Framework analysis:** based on the results of Step 1, governments should consider which elements of the Framework would be more relevant and applicable to the specific threat assessment.
- **Step 3. FCCs identification and assessment:** building on Step 2, once the most relevant elements of the Framework have been identified based on national threat assessment, governments can use the list of FCCs to identify specific capabilities required to address specific threats. Once this identification is completed, it can become a useful baseline to assess the extent to which a given State could leverage the Framework to prevent or respond to specific threats.

This approach is illustrated with the use of three scenarios: two focusing on different types of malicious acts (ransomware and distributed denial of service) and one focusing on a specific vector (supply-chain tampering).

Independently from the threat profile, certain norms and associated foundational capabilities should be considered relevant and applicable no matter the scenario or threat under consideration—specifically Norm A on inter-State cooperation, and Norm E on human rights. The analysis of the three scenarios builds upon this point and identifies additional specific foundational cyber capability elements that appear to be recurring across multiple threats and across multiple norms.

From a policy and regulation perspective, States should prioritize the development (and periodic review) of comprehensive national cyber security strategies and policies which, in combination with adequate laws, enable States to take all the necessary steps domestically and internationally for ensuring the protection of the ICT domain, including via multi-Stakeholder cooperation. In addition, States should prioritize the development of comprehensive and public-facing positions on how international law applies to the ICT domain.

From a process perspective, States should prioritize the development of mechanisms to facilitate cooperation on matters pertaining to ICT security with all relevant national stakeholders, including government agencies, private sector, the technical community and civil society as appropriate. This would ensure not only timely, efficient and effective information flows in time of crisis, but also access to knowledge assets that can be leveraged as appropriate to compensate for potential shortages or lack of

available expertise in the public sector. Similarly, States should develop mechanisms to facilitate cooperation and information at the bilateral, regional and international levels. The development of dedicated processes and mechanisms would enable the creation of **functioning partnerships and networks.**

In relation to structures, States should prioritize the development and sustainability of fully operational national **computer incident response capabilities** which are irreplaceable elements of the first line of defence against malicious ICT acts. Various arrangements between public and private CSIRTs/CERTs could be explored at the national and regional levels to account for limitations in resources, skills or technologies. In addition, States should priorities the identification of a **responsible agency** within the national government to act as **focal points for ICT issues at the political and technical levels**, including with the creation of a dedicated National Point of Contact. The presence of an **agency with the authority and powers to investigate and prosecute** malicious ICT acts appears to be a cross-cutting requirement.

While all sectors are suffering from a cyber skills shortage, the successful implementation of the Framework will be based on the ability of States to develop internally, or access through external partnerships, **adequate technical and legal expertise** to be able to manage effectively ICT incidents domestically and ensure compliance with the Framework, but also to engage constructively with counterparts at the international level on issues pertaining to ICT security. This will become an increasing demand on diplomats as well, who should strengthen their understanding of ICT issues and be supported by specialists and advisors as necessary.

Finally, the successful implementation of the Framework will rely also on a State's ability to access a certain number of **technologies and technical solutions** either by developing them nationally or by accessing them through partnerships with others (e.g., bilateral or regional agreements with other States, or public–private partnerships). These technological solutions include, but are not limited to, **capabilities to prevent, detect, and disrupt different types of attack** (e.g., threat intelligence platforms, early warning systems) and solutions to increase the confidentiality, integrity and availability of systems and data (e.g. cloud-based data centres).

1. Introduction

The socioeconomic advantages and opportunities brought by the rapid and widespread development of information and communication technologies (ICTs) carries new risks and threats for Member States and the international community at large. As highlighted in the final reports of the 2019–2021 Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, and the Group of Governmental Experts (GGE) on advancing responsible State behaviour in cyberspace in the context of international security, harmful ICT incidents are increasing in frequency and sophistication, and are constantly evolving and diversifying. The first annual progress report of the 2021–2025 OEWG also emphasized the increased threats posed by ICTs to critical infrastructure and services, and the risk posed by novel and emerging technologies.

In the fourth substantive session of the OEWG 2021–2025, held in March 2023, more than 60 delegations took the floor to speak on the issue of existing and potential threats, the highest number ever of contributions on this specific agenda item. The combination of (1) heightened geopolitical tensions, (2) reported malicious ICT activity by State actors, (3) serious ICT incidents perpetrated by sophisticated criminal groups targeting both public services and critical infrastructure operated by private

sector, and (4) the increased awareness of the impact of emerging technologies such as artificial intelligence (AI) and quantum computing, have increased both the depth and breadth of discussions held by States related to threats.

Nevertheless, the extent to which such discussions are linked to the broader context, scope and purpose of the OEWG remains limited. As States discuss the four key pillars of the Framework of responsible State behaviour in the use of ICTs (henceforth, the Framework)—norms of responsible behaviour, international law, confidence-building measures and capacity-building—two key aspects remain under-explored:

a. the extent to which the implementation of the Framework can be used to increase national, regional and international security and resilience against specific threats; and
b. how specific threats can be used to inform capacity-building initiatives.

This report is the second of a two-part study conducted by UNIDIR that aims at strengthening the linkages between the Framework and States' ability to effectively prevent or mitigate the impact of selected malicious ICT activities by designing a tool to better identify requirements and prioritize capacity-building interventions.

This report is centred on the concept of Foundational Cyber Capabilities (FCCs) as introduced and described in the first report of this study.[1]

1 See Samuele Dominioni and Giacomo Persi Paoli. 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping Foundational Cyber Capabilities. UNIDIR.

2. Recap of Key Concepts

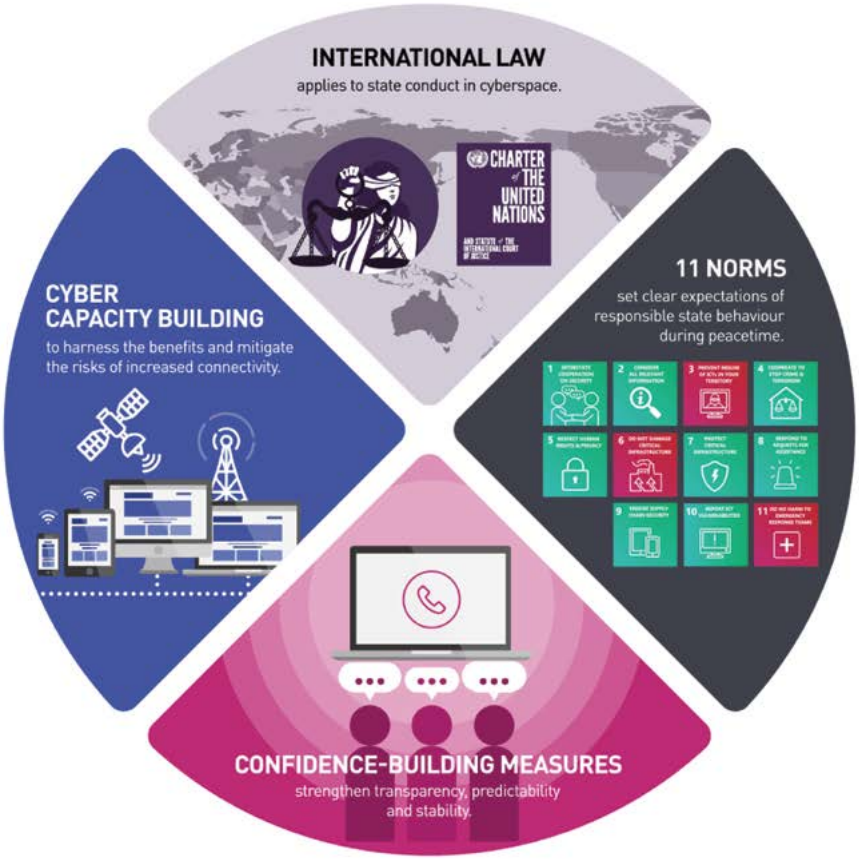
2.1 The Framework of Responsible State Behaviour in the Use of ICTs

For the last two decades, Member States have been discussing the use of ICTs in the context of international peace and security. Following the GGE of 2015, a set of 11 voluntary, non-bindings norms of responsible State behaviour was developed and adopted by the General Assembly,[2] and further refined in subsequent multilateral processes.[3] These norms, combined with the reaffirmation that international law is applicable to the ICT domain, with dedicated confidence-building measures (CBMs) and targeted capacity-building and cooperation initiatives, form the elements of the Framework for Responsible State Behaviour in cyberspace (see figure 1).

2 See A/RES/70/237.

3 See OEWG 2021 Final Substantive Report, and GGE 2021 Report.

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



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

A key component of the Framework are the 11 voluntary norms. These tackle a wide range of issues pertaining to international cybersecurity and indicate behaviours that States should and should not undertake in their use of ICTs to preserve peace and security in the ICT domain. Table 1 provides an overview of the 11 norms.

Table 1. Norms of Responsible State Behaviour in Cyberspace[4]

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

4 Icons from: https://www.internationalcybertech.gov.au/un-cyber-norms-resources.

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.

Norm G

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

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.

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.

Norm J

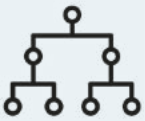
States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

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.

2.2 Foundational Cyber Capabilities[5]

Foundational Cyber Capabilities (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:

Policies and Regulations 	Official documents related to cybersecurity matters. These include documents outlining Member States' positions, policies, strategies (de-veloped 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.
Processes and Structures 	Key positions, responsible agencies/entities, other national or regional mechanisms, and official processes, procedures and protocols related to cybersecurity.
Partnerships and Networks 	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.
People and Skills 	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.
Technology 	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.

5 This section is an extract of the first part of this study presented in Samuele Dominioni and Giacomo Persi Paoli. 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping Foundational Cyber Capabilities. UNIDIR.

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 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 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. An overview of the full list of FCCs for each element of the Framework can be consulted in Annex A and more detailed explanations of each FCC are provided in the first report of this study.[6]

6 Samuele Dominioni and Giacomo Persi Paoli. 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping Foundational Cyber Capabilities. UNIDIR.

3. Introducing the Threat-Based Approach

As mentioned in Chapter 1, the threat landscape in the ICT domain is constantly evolving, becoming more complex and sophisticated as the baseline of cybersecurity measures becomes higher and higher. While it should be noted that more than 90 per cent of cyberattacks could be prevented[7] by the systematic application of basic security 'hygiene' (e.g., change default passwords, use multi-factor authentication, use anti-malware, install security updates promptly, etc.), the Framework for responsible State behaviour can provide an important additional layer of resilience. Indeed, putting in place the capabilities necessary to implement the Framework would equip States with important tools that can contribute to the prevention or mitigation of specific cyber threats as well as to the strengthening of their overall cyber resilience.

---

7 Different estimates exist by a number of cybersecurity and technology company. For example, the Microsoft Digital Defense Report released in November 2022 estimates that basic security hygiene still protects against 98 per cent of attacks; see https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.

In the last decade, several methodologies, models, and approaches have been developed and successfully deployed to identify what elements and steps governments should undertake to develop or strengthen their national ICT capabilities.[8] However, no existing model specifically addresses the implementation of the Framework while considering different national contexts and different threat perceptions.

In this context, this research project 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. The proposed 'threat-based approach' encompasses three steps:

- **Step 1. Threat and risk assessment:** in this step, a given government should map, assess and prioritize ICT threats that are affecting its territory. To carry out this analysis governments can rely on domestic sources (e.g., threat intelligence reports from its cybersecurity agency/entities), and/or other sources (e.g., threat intelligence reports provided by private companies). The threat should take into consideration not only the type of attack or malware used, but also wider elements such as the most vulnerable or exposed targets, the different types of threat actors, the potential cross-border nature of the threat itself or of the potential response, and others. It is important that such threat assessments consider also risk scenarios in which the country is not necessarily the intended victim of the attack, but perhaps serves as instrumental victim, for example as a 'transit' or routing country for an attack intended for someone else. An example of a tool that governments could use to conduct a comprehensive threat and risk assessment is UNIDIR's Taxonomy of Malicious ICT Incidents.[9]
- **Step 2. Framework analysis:** based on the results of Step 1, governments should consider which elements of the Framework would be more relevant and applicable to the specific assessment. It is important to recognize that each threat or ICT incident, even of the same type, while having certain commonalities, would also be characterized by unique factors. However, when looking at more general threat profiles and not at specific and unique incidents, it would be possible to identify which norms, elements of international law and confidence-building measures would be more relevant.
- **Step 3. FCCs identification and assessment:** building on Step 2, once the most relevant elements of the Framework have been identified based on national threat assessment, governments can use the list of FCCs (see Annex A) to identify specific capabilities required to address specific threats. Whether all FCCs listed under each element of the Framework or only a selection of them would be applicable would depend on specific threat under consideration. Once this identification is completed, it can become a useful baseline to assess the extent to which a given State could leverage the Framework to prevent or respond to specific cyber threats.

---

8 See the **Oxford Cybersecurity Capacity Maturity Model for Nations** (CMM) and the **International Telecommunication Union Global Cybersecurity Index survey**.

9 Samuele Dominioni and Giacomo Persi Paoli. 2022. A Taxonomy of Malicious ICT Incidents. UNIDIR. **https://unidir.org/publication/taxonomy-malicious-ict-incidents**.

In addition to informing capacity-building priorities by giving another perspective on possible gaps and needs, this methodology also brings two additional benefits. First, it could be used by governments to conduct regular 'health checks' of their cybersecurity architectures to ensure that they remain fit for purpose as threats evolve. Second, it could be used to conduct periodic table-top, scenario-based exercises (at the national or regional level) involving all relevant stakeholders to examine the readiness and resilience to prevent or manage both existing and potential new threats.

It should be noted that this approach is not meant to rank components of the Framework, or even norms themselves, by importance. All components of the Framework are essential and should be taken into consideration. Nevertheless, when looking at specific threat scenarios, different capabilities might be more relevant or applicable than others to deal with specific circumstances. Some capabilities may even be prerequisites for others.

Finally, it is important to highlight that the factors beyond the list of FCCs, which was developed exclusively with a focus on the Framework, will ultimately impact the capability of a State to prevent or mitigate cyber threats. However, as mentioned earlier in this section, developing or strengthening the capabilities to implement the Framework will contribute positively to the overall cyber resilience of a State.

4. The Threat-Based Approach in Action: Illustrative Examples

To develop the threat-based approach and illustrate how it can be used to identify specific capability requirements, three different threat scenarios were developed by the project team and used to conduct dedicated workshops with internal and external experts.[10]

Based on the analysis of the most recent discussions on existing and emerging threats in the context of the OEWG, three specific cyber threats were selected as illustrative examples for this methodology:

---

10 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, elements of international law, or confidence-building measures that could be applicable to the scenario. Then, they selected the most suitable FCC elements to address the threat. 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. Subsequently, additional checks on the findings were conducted with external experts.

two focusing on different types of malicious acts (malware and distributed denial of service) and one focusing on a specific vector[11] (supply-chain tampering). In particular, the malicious ICT acts proposed for this study are the following.

a. **Malware operations targeting data** (e.g., ransomware, data wipers): malicious software that seeks to undermine data confidentiality, integrity, or availability. Ransomware is a type of malware that seeks to encrypt data or threatens to leak exfiltrated data to obtain a ransom payment. A wiper is a class of malware intended to erase ('wipe', hence the name) the hard drive of the computer it infects, maliciously deleting data and programs.
b. **Distributed Denial of Service (DDOS) act:** a type of cyber operation in which a malicious actor aims to render a computer, device, or network unavailable by interrupting the device's normal functioning by overwhelming it with system requests until normal traffic is unable to be processed, resulting in denial-of-service.
c. **Software supply-chain tampering:** an act that injects malicious code into an application or software to infect all users. In software supply-chain tampering, malicious actors seek to leverage trusted relationships between clients and vendors, who may be unaware that their software is infected with malicious code when they are release it to the public. The malicious code then runs with the same trust and permissions as the original software it is attached to.

In addition to the specific nature of the malicious act, the three threat scenarios include variations of other key factors: **types of victims** (e.g., critical infrastructure operators, government agencies, other private sector actors and users), uncertainty over the **involvement of State actors as perpetrator** and **cross-border dimensions** of the incident. There is no standard or recommended list of factors to consider when thinking about threats. UNIDIR's taxonomy of malicious ICT incidents offers a good overview of what these factors might be, but it is ultimately a choice that is dependent on national or regional contexts.

To add more realism to the exercise and stimulate more specific discussions, the three threat profiles were further developed into short scenario narratives, based on real events, that were used to describe a specific (although hypothetical) cyber incident.

It should be noted that irrespective of the threats, some elements of the Framework, and associated capabilities, should be considered as always applicable. These are Norm A and Norm E:

11 "Vector" refers to the method of intrusion into a system or a network; see Samuele Dominioni and Giacomo Persi Paoli. 2022. A Taxonomy of Malicious ICT Incidents. UNIDIR. https://unidir.org/publication/taxonomy-malicious-ict-incidents.

	**Norm A**
	This norm is always applicable given its high-level/strategic nature which underpins any form of cooperation among States on international ICT security and its implementation includes foundational elements, such as Computer Security Incident Response Teams (CSIRTs) / Computer Emergency Response Teams (CERTs), which are critical to ensure national cyber resilience.
	**Norm E**
	This norm is always applicable as respect for human rights underpins States' behaviour in the ICT domain no matter the threat scenario.

Finally, it is worth noting that several FCCs are repeated across multiple scenarios, sometimes with more specific nuances, sometimes as identical requirements. This is due to the fact that each scenario is intended to be readable as a stand-alone section and thus all relevant information is provided.

4.1 Scenario 1: Ransomware

Threat Profile

Type	Ransomware
Victim	Two energy sector critical infrastructures
Perpetrator	Criminal group with possible involvement of a State actor
Cross-border	Yes; the headquarters of the infrastructures are located in two different countries, and evidence suggests the involvement of two different perpetrators, both based in third countries

Scenario Description

In this scenario, perpetrators employed ransomware to conduct a malicious ICT act targeting two transnational critical infrastructures in the oil and gas industry, with their headquarters in two different countries (Country Alpha and Country Beta). This act led to a 60 per cent reduction in the distribution of oil and gas in Country Alpha. The ransom note demanded payment of USD 10 million. Preliminary analysis conducted by cybersecurity companies suggested that the act was launched by a criminal hacking group largely operating from third country (Country Charlie). Subsequently, additional forensic analysis conducted by the cybersecurity law enforcement unit of Country Alpha found that the malware showed a level of sophistication and some specific markers associated with the cyber capabilities, tactics, techniques and procedures of another country, Country Zero, although evidence was not conclusive. Country Alpha and Country Zero have a history of difficult diplomatic relationships due to conflicting geostrategic interests.

Elements of the Framework Relevant to the Scenario

Based on research and consultation with experts, the following components of the Framework have been considered particularly relevant for this scenario:

	**Norm B**
	Given the complexity of the scenario, the uncertainty over the perpetrator and the possible involvement of Country Zero, and the wider geopolitical context, Norm B is particularly relevant for both victim States (Alpha and Beta) who may wish to attribute the attack to a specific actor.
	**Norm C**
	In the scenario, initial evidence suggests that the perpetrator, a criminal hacking group, was operating from Country Charlie. As such, Norm C becomes highly relevant for Country Charlie who will be expected to act in compliance with this norm.

Norm D

In order to be able to take action in response to the information available which points to the possible involvement of a criminal group based in Country Charlie, it is important that targeted countries (Alpha and Beta) and Country Charlie are equipped with the necessary capabilities to implement Norm D and thus to cooperate.

Norm F

Given the target of this attack, and the possible role played by Country Charlie and Country Zero, Norm F is also highly relevant.

Norm G

Mirroring the consideration made for Norm F, Norm G becomes highly relevant for Countries Alpha and Beta whose critical infrastructure has been targeted.

Confidence-Building Measures

Given the transnational dimension of the incidents, and the possible involvement of two other countries, the ability to implement CBMs supporting communication and transparency among States is particularly relevant.

International Law

Most of the norms considered relevant for this scenario require for their implementation the formulation of clear national interpretations of legal concepts (e.g., due diligence, critical infrastructure, the principle of non-intervention).

Relevant FCCs Applicable to the Scenario

Policies and Regulations	• Regarding **policies and regulations** relevant to this scenario, all countries involved should have elaborated a **national interpretation of all the norms concerned** and their **understanding of how international law (IL) applies to the ICT domain.** • Country Alpha should have a policy that outlines the **methodology and definitions for its attribution** process (Norm B). • Given the different stakeholders involved in the incident, **frameworks allowing for the exchange information** with relevant commercial and other non-governmental stakeholders are particularly important (Norms D, G). • Considering the role of a criminal group in the scenario, countries involved in the incidents should have **appropriate strategies, policies and legislations** in place that **set provisions to prevent, detect, and interrupt malicious use of ICTs** (Norm C) and that **enable the cooperation** in investigation and prosecution of cyber-criminal activity (Norm D). Given the specific nature of the attack, such policies and strategies should also cover the topic of data security to ensure that proper measures can be implemented to create backups and redundancies. • Countries Alpha and Beta (targeted countries) should have **designated critical infrastructure sectors and passed legislation on the protection of critical infrastructure** (Norm G). • Finally, governments of Country Charlie and Country Zero should be able to demonstrate that their **national policies and legislations are aligned with the Norm F** and the requirement to not damage critical infrastructure. At the very least, their **own public interpretation of the norm would be needed.**
Processes and Structures	• Countries Alpha and Beta, as targeted countries, should develop **national standards of proof of attribution** (Norm B), as well as processes and procedures to enable **information-exchange and cooperation among relevant governmental and non-governmental entities** across all countries involved, including protocols especially for digital evidence (Norms A, B, C, D, G). • In terms of structures, Countries should have well-established and fully-operational **national or regional CSIRTs/CERTs** (Norms A, C, D, G, CBMs) as well as **Points of Contact both at the diplomatic and technical level** (Norm A, CBMs) and an **independent and effective oversight mechanism** capable of ensuring transparency and accountability for State operation (including on data collection) in the ICT domain (Norms A, E, F and IL).

Partnerships and Networks	• Within targeted countries, intersectoral cooperation, including with the private sector, would key to properly resolve and recover from the malicious ICT act (Norms A). This should include **cross-border cooperation with relevant infrastructure owners and operators** (Norm G). • Among targeted countries, **bilateral cooperation to ensure information-exchange** (as per Norms A, B, C, and F) and **cross-border investigations** (Norm D) would be essential. • **Bilateral cooperation** would also be important between targeted countries (Alpha and Beta) and countries potentially involved in the malicious act (Charlie and Zero) with a specific focus on the **settlement of disagreements and disputes** (as per Norm B) and on **investigation** (as per Norm D).
People and Skills	• To adequately respond to the scenario, targeted Countries Alpha and Beta would require experts with skills to **manage cybersecurity incidents** (Norm A) and to **conduct or appraise technical investigations** of ICT incidents (Norm B). Country Charlie would also require expertise in the **identification and disruption of malicious ICT acts** emanating from its own territory (Norm C). • In addition to technical and incident management skills, it is important that all governments involved have access to **legal expertise** on the applicability of international law in the ICT context (Norms A, B, F, and IL) as well as adequate **negotiation and public communication skills** specific to the ICT context and critical infrastructure (Norms B, C, G and CBMs).
Technology	• Based on the scenario, both targeted countries as well as the country from which the suspected cyber-criminal group is operating should be equipped with **technical capabilities to prevent, detect, and disrupt malicious ICT acts**, particularly against critical infrastructure (Norms A, C, D, G). The countries targeted by ransomware would also require technological solutions to ensure redundancy and backup of data (e.g. cloud-based data centres)

4.2. Scenario 2: Distributed Denial of Services (DDoS)

Threat Profile

Type	Distributed Denial of Service (DDOs)
Victim	Government websites and applications
Perpetrator	An Advanced Persistent Threat (APT) with plausible involvement of a State actor
Cross-border	Yes; attacks have been routed through multiple countries

Scenario Description

Country Alpha suffered a prolonged campaign of multiple DDoS attacks targeting its public services (including social security systems). Early investigations of the incidents highlighted that the malicious acts were routed through computers and networks in two other countries (Beta, Charlie). As the DDoS attacks increased in frequency and magnitude, Country Alpha declared a state of emergency. Additional investigations by Country Alpha authorities linked the malicious ICT acts to a known APT closely associated with the government of a third country with competing strategic interests (Country Zero).

Elements of the Framework Relevant to the Scenario

Based on research and consultation with experts, the following components of the Framework have been considered particularly relevant for this scenario:

Norm B

In this scenario, to combination of the routing of the attacks through third countries, the potential involvement of an APT associated with another State and the seriousness of the impact that led to the declaration of national emergency, may bring the victim (Country Alpha) to consider the option of publicly attributing the attack to another State. In this case, Norm B is particularly pertinent.

Norm C

This norm is particularly relevant to the 'transit countries' in this scenario who play a key role in the disruption of the attack.

Norm D

To effectively respond to this threat scenario, the victim country and the transit countries should be able to effectively implement the norm that calls for cooperation to stop the malicious activities perpetrated by the APT.

	**Confidence-Building Measures**
	Given the transnational dimension of the incidents, the effective implementation of CBMs, particularly of a well-established and fully operational Points of Contact at the diplomatic and technical levels, would be particularly relevant in managing both the operational and political responses to the incident.
	**International Law**
	The threat scenario presented in this case, along with the norms highlighted as relevant, require involved countries to elaborate clear positions on key international law issues such as due diligence, the principle of non-intervention, and the principle of State responsibility.

Relevant FCCs Applicable to the Scenario

Policies and Regulations	• Regarding policies and regulations, as a starting point, countries should have **national interpretations of the components of the Framework applicable to this scenario** (Norms B, C, D, and IL). This will provide the basis upon which to build the specific response. • Additionally, there are several policies and regulations that countries should have adopted/implemented depending on their role in the scenario. For what concerns Norm B on attribution, Country Alpha, as the victim country, should have a **classification of ICT incidents in terms of scale and impact** that could underpin the declaration of the state of emergency and a **policy on attribution**, including on definitions and the methodology. • Norm C is particularly relevant for transit countries, which should have **cybersecurity policies and strategies that outline provisions to prevent, detect, and interrupt malicious ICT acts**, supported by adequate **legislative measures to investigate and prosecute** those acts (Norms C, D). • All countries involved should also have established **regulations allowing cooperation and information-exchange** with relevant commercial and non-governmental entities (Norm D).

Processes and Structures	• There are several processes and structures relevant to this scenario. In terms of processes, to support the possible attribution of the incident to a third country (Norm B), Country Alpha should develop **national standards of proof, and processes and procedures** (including protocols especially for exchanging digital evidence) **to enable information-exchange** among relevant governmental and non-governmental entities (Norms B, C, and D). • In terms of structures, countries should have working **national or regional CSIRTs/ CERTs** (Norms A, C, D). • Given the transnational dimension of the DDoS attacks, it is also crucial that countries Alpha, Beta and Charlie have **cyber-law-enforcement capacities** (Norms C, D), as well as **cooperation mechanisms** among them (Norm A) to promptly intervene and disrupt the malicious activities. • **National Points of Contact** both at the diplomatic and technical levels (Norm A, CBMs) would play a key role in the management and resolution of the incident. • Finally, all States involved should have an **independent and effective oversight mechanism** capable of ensuring transparency and accountability for State operation (including on data collection) in the ICT domain (Norms A, E, and IL).
Partnerships and Networks	• To manage a comprehensive attack on public institutions, **intragovernmental cooperation and multi-stakeholder cooperation** would be required (Norms A, C). • **International cooperation** focused on **information-exchange** (Norms A, B, C) and **investigation and prosecution** (Norm D) between countries Alpha, Beta and Charlie would be essential and would require the availability of **cooperation protocols and mechanisms.** • At the same time, it is crucial that **bilateral cooperation and communication,** via **Points of Contact** and diplomatic channels would be required between Country Alpha and Country Zero to manage the political implications of the incident and work towards the settlement of disagreements and disputes (CBMs).
People and Skills	• To adequately respond to the scenario, the target country Alpha would require experts with skills to **manage cybersecurity incidents** (Norm A) and to **conduct or appraise technical investigations** of ICT incidents in support of the implementation of Norm B. Countries Beta and Charlie would also require expertise in the **identification and disruption of malicious ICT acts** emanating from their own territory (Norm C). • In addition to technical and incident management skills, it is important that all countries involved have access to **legal expertise** on the applicability of international law in the ICT context (Norms A, B, F, and IL) as well as adequate **diplomatic and public communication skills** specific to the ICT context to effectively manage both the bilateral relations with other countries involved and more general public communication with other countries and stakeholders (Norms B,C, G and CBMs).

Technology	• The technological elements relating to this scenario concern **capabilities to prevent, detect, and disrupt** the DDoS attacks in the victim country as well as in the countries of transit (Norm A). These could include, for example, Content Delivery Network solutions to help absorb and deflect a DDoS attack by distributing traffic across multiple servers to mitigate the impact of an attack and prevent a single point of failure, or cloud-based DDoS Protection Services to detect and mitigate attacks in real time, leveraging the scalability of the cloud to handle large-scale attacks.

4.3. Scenario 3: Supply-Chain Tampering

Threat Profile

Type	Malware (supply-chain backdoor)
Victim	A cybersecurity software provider and thousands of users, including public institutions
Perpetrator	Unknown but plausible State actor
Cross-border	Yes; victims are distributed across the world and the intrusion was routed through servers in multiple countries

Scenario Description

A cyber security company based in Country Alpha discovered malware that had infected a vast number of customer systems. The malware appeared to have been delivered through a supply-chain tampering act that targeted a third-party software provider (headquartered in the same country) who inadvertently distributed the backdoor malware through a scheduled software update. More than 50,000 public and private organizations across the world use the software in question as an enterprise management tool. As a result, the attack compromised the data, networks, and systems of thousands of organizations and users and potentially exposed their customers and partners as well. Analyses conducted by authorities of a group of countries suggested that by managing the intrusion through multiple servers based in different countries and mimicking legitimate network traffic, the perpetrators were able to circumvent threat detection techniques employed by both private companies and government agencies, denoting a level of sophistication typical of an advanced State actor.

Elements of the Framework relevant to the scenario

Based on research and consultation with experts, the following components of the Framework have been considered particularly relevant for this scenario:

Norm D

The malware targeted a software provider in Country Alpha, but the impact was worldwide, calling for inter-State cooperation in the investigation and prosecution of the incident.

Norm G

Given the vast scale and impact of the malicious act, ensuring the protection of critical infrastructure from supply-chain risks is essential.

	**Norm I** Given that the scenario is based on a compromised software supply chain, this norm is indeed central to the scenario.
	**Confidence-Building Measures** Given the transnational dimension of the incidents, CBMs particularly designed with the goal of supporting more efficient communication and exchange of information among States are particularly relevant.
	**International Law** Despite the lack of sufficient evidence to attribute the attack to a specific perpetrator, the threat scenario presented in this case, along with the norms highlighted as relevant, require involved States to elaborate clear positions on key international law issues such as due diligence (particularly Country Alpha), the principle of non-intervention, and the principle of State responsibility.

Relevant FCCs applicable to the scenario

Policies and Regulations	• All countries involved in the incident should have adopted and implemented **policies and strategies to prevent, detect, and interrupt malicious ICT acts**, supported by adequate **legislative measures to investigate and prosecute those acts** (Norm D). • All countries involved should also have established **regulations allowing cooperation and information-exchange** with relevant commercial and non-governmental entities (Norms D). • To safeguard critical infrastructure, countries should have a **national designation of critical infrastructure**, cybersecurity policy or strategy with **provisions on cyber risk reduction, cybersecurity measures for ICT products supporting critical infrastructure operations** and all other measures included in resolution 58/199 on the global culture of cybersecurity and critical information infrastructure protection (Norm G). • Moreover, in their cybersecurity policy or strategy, countries should address **supply-chain risk** and provide an **appropriate framework** to prevent and mitigate it (Norm I). Related to this point could be the development and implementation of **common rules and standards for supply-chain security** (although this goes beyond the scope of what is achievable by a single country). • Other key elements relevant to this threat scenario are the development of **regulations** prohibiting the introduction of harmful hidden functions and exploitation of vulnerabilities in ICT products and the development of **strong supply-chain security requirements for vendors** to be incorporated into the life-cycle management of safety and ICT products (Norm I).

Processes and Structures	• Particularly important for this scenario would be for all involved countries to develop and implement a **supply-chain risk governance mechanisms** involving key stakeholders representing every node of the value chain to coordinate actions and responses to the malicious act (Norm I). • Moreover, to support effective communication between governmental and non-governmental stakeholders (Norm C), countries should develop and implement **processes and procedures (including protocols especially for exchanging digital evidence) to enable information-exchange** (Norm D). This should include processes to acquire, process, and store data and information for cyber investigation and prosecution. • In terms of structures, it is important to establish Points of Contact at the diplomatic and technical levels (Norm A) to enable governments of the countries involved to maintain open and efficient channels of communication. • Countries should also have working **national (or regional) CSIRTs/CERTs** (Norms A, D, G) to mitigate the impact and minimize the recovery time after the incident and such CSIRTs/CERTs should be well coordinated. • In addition to the technical coordination among CSIRTs/CERTs, it is important for countries to have designated **national agencies with the legal power to investigate, prosecute and enforce the rule of law in relation to malicious acts in the ICT domain.** These agencies should be able to effectively interact and cooperate with each other as needed (Norms A, D). • Finally, an independent and effective **oversight mechanism** that ensures transparency and accountability for State operation (including data collection) in the ICT domain is also essential (Norms A, E).
Partnerships and Networks	• For what concerns partnerships and networks, there are important elements that countries should set up to address supply-chain tampering threats. **Intersectoral cooperation among national agencies and the private sector** (in the scenario: the cybersecurity firm, the software provider, and other relevant stakeholders) is key to properly responding to supply-chain attacks targeting, for example, automatic security update processes (Norms A). • Moreover, **bilateral, regional, and multilateral cooperation between States** for information-exchange for investigation (including through technical and law enforcement networks) and prosecution (Norms A, D), and for knowledge-exchange on measures to ensure the integrity of the supply chain (Norm I) are essential.

People and Skills	• To adequately respond to the scenario, all targeted countries would require experts with skills **to manage cybersecurity incidents** (Norm A) in particular those resulting from a compromised supply chain (Norm I) and with a view to maximizing the efficiency of the response and recovery phase. • In addition to technical and incident management skills, it is important that all countries involved have access to **legal expertise** on the applicability of international law in the ICT context to ascertain possible legal implications of the incident (Norm A), as well as adequate **diplomatic and public communication skills** specific to the ICT context, particularly from the country where the attack originated, to effectively manage both the bilateral relations with other countries involved and more general public communication with other countries and stakeholders (Norm I).
Technology	• Targeted countries and organizations should be equipped with, or have access to via an external partner, the **technical capability to prevent, detect, or disrupt supply-chain attacks** (Norm I). These capabilities may include, but are not limited to, threat intelligence platforms, early warning systems, and ideally tools for the assessment of ICT products.

5. Conclusion

The three examples presented in Chapter 4 provide an illustration of how specific measures designed to implement the Framework for Responsible State Behaviour in cyberspace could contribute to preventing, or managing and strengthening the response to a selection of malicious ICT acts and, by extension, reinforce national cyber resilience overall.

It is important to recall not only that these are illustrative examples, but that important elements of national cyber preparedness and maturity may not be directly associated with the Framework and therefore have not been included in the list above. Nevertheless, the purpose of this report is to demonstrate—as a complement the more holistic assessment of national implementation of the Framework presented in Part I of this study[12]—how a more focused approach based on specific threat profiles may add an additional layer of analysis that can further refine a State's understanding of its current cyber capabilities.

In the preamble to Chapter 4, it is noted how—independently from the threat profile—certain norms and associated foundational capabilities should be consider relevant and applicable no matter the

12 See Samuele Dominioni and Giacomo Persi Paoli. 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping Foundational Cyber Capabilities. UNIDIR.

scenario or threat under consideration. This refers to Norm A on inter-State cooperation, and Norm E on human rights. The analysis of the three scenarios builds upon this point and identifies additional specific FCCs that appear to be recurring across multiple threats and across multiple norms.

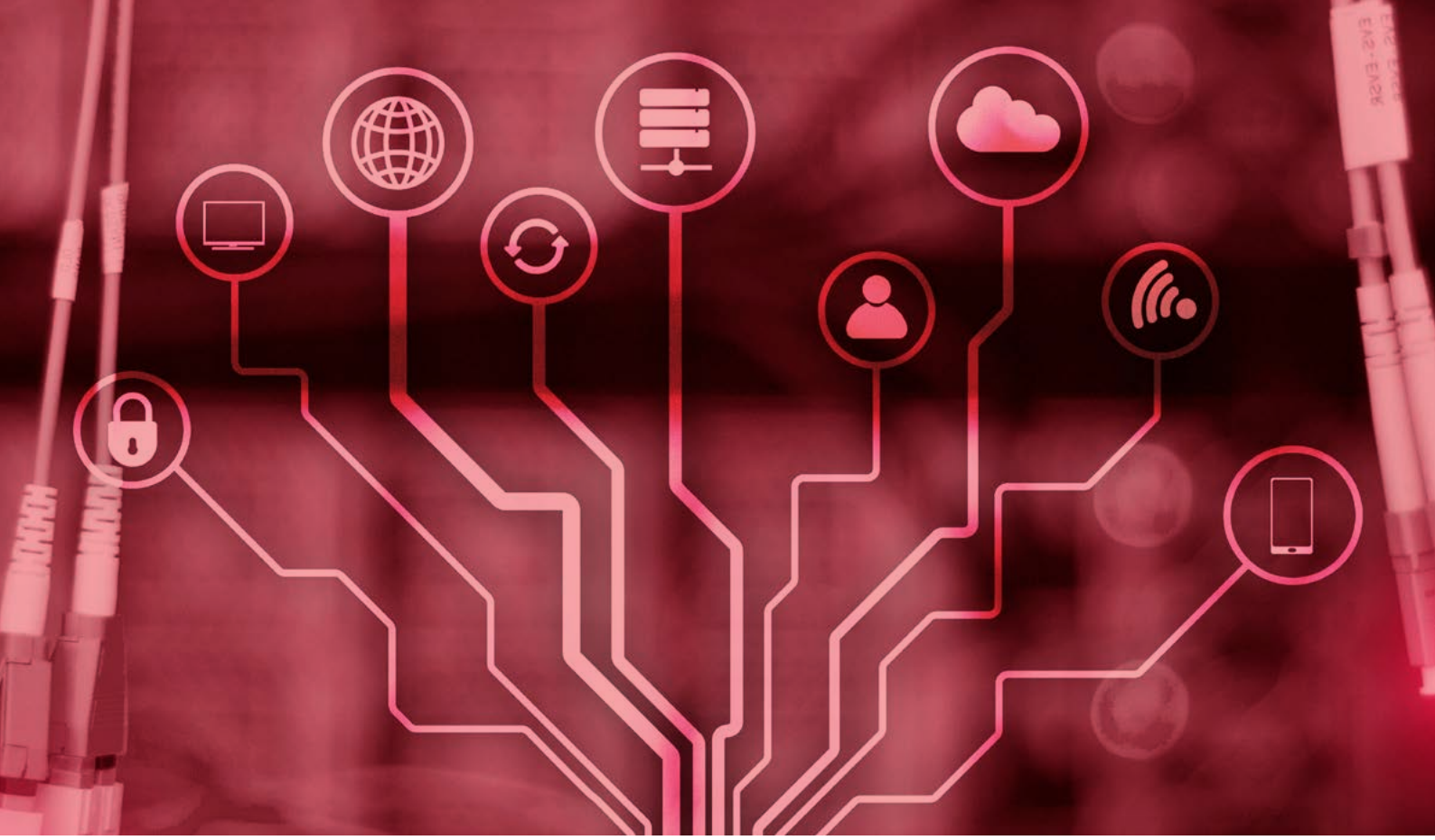
From a policy and regulation perspective, States should prioritize the development (and periodic review) of comprehensive national cyber security strategies and policies which, in combination with adequate laws, enable States to take all the necessary steps domestically and internationally for ensuring the protection of the ICT domain, including via multi-stakeholder cooperation. In addition, States should prioritize the development of comprehensive and public-facing positions on how international law applies to the ICT domain.

From a process perspective, States should prioritize the development of mechanisms to facilitate cooperation on matters pertaining to ICT security with all relevant national stakeholders including government agencies, the private sector and technical community, and civil society as appropriate. This would ensure not only timely, efficient and effective information flows in time of crisis, but also access to knowledge assets that can be leveraged as appropriate to compensate for potential shortages of available expertise in the public sector. Similarly, States should develop mechanisms to facilitate cooperation and information-exchange at the bilateral, regional and international levels. The development of dedicated processes and mechanisms would enable the creation of **functioning partnerships and networks.**

In relation to structures, States should prioritize the development and sustainability of fully operational national **computer incident response capabilities** which are irreplaceable elements in the first line of defence against malicious ICT acts. Various arrangements between public and private CSIRTs/CERTs could be explore at the national and regional levels to account for limitations in resources, skills or technologies. In addition, States should prioritize the identification of a **responsible agency** within the national government to act as **focal points for ICT issues at the political and technical levels**, including with the creation of a dedicated National Point of Contact. The presence of an **agency with the authority and powers to investigate and prosecute** malicious ICT acts appears to be a cross-cutting requirement.

While all sectors are suffering from a cyber skills shortage, the successful implementation of the Framework will be based on the ability of States to develop internally, or access through external partnerships, **adequate technical and legal expertise** to be able to manage effectively ICT incidents domestically and ensure compliance with the Framework, but also to engage constructively with counterparts at the international level on issues pertaining to ICT security. This will become an increasing demand on diplomats as well, who should strengthen their understanding of ICT issues and be supported by specialists and advisors as necessary.

Finally, the successful implementation of the Framework will rely also on a State's ability to access a certain number of **technologies and technical solutions** either by developing them nationally or by accessing them through partnerships with others (e.g., bilateral or regional agreements with other States, or public–private partnerships). These technological solutions include, but are not limited to, **capabilities to prevent, detect, and disrupt different types of attack** (e.g., threat intelligence platforms, early warning systems) and solutions to increase the confidentiality, integrity and availability of systems and data (e.g. cloud-based data centres).



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).

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.

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.

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.

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

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	

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.

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.

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: • 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: • 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

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG