ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace

Acknowledgments

ASEAN Member States would like to acknowledge the support provided by the UN Office for Disarmament Affairs (UNODA) in the development of the ASEAN Checklist for the implementation of the Norms of Responsible State Behaviour in Cyberspace and the Security and Technology Programme at the United Nations Institute for Disarmament Research (UNIDIR) for the finalization of it.

Contents

Introduction

The 11 voluntary, non-binding norms of responsible State behaviour in cyberspace were first agreed upon by the 2015 United Nations group-of-governmental experts in 2015, and subsequently endorsed by consensus at the General Assembly in 2015 through resolution 70/237. In 2018, ASEAN ministers responsible for cybersecurity subscribed in principle to the 11 cyber norms, and expressed ASEAN's commitment to operationalize the norms to promote regional stability in cyberspace. The 11 cyber norms were also reaffirmed at the Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies 2019–2021, and 2021–2025.

While the 11 norms outline the broad principles of responsible behaviour in cyberspace through high-level statements, the Norms Implementation Checklist (NIC) provides a set of actions that all States can consider and follow to implement the United Nations norms of responsible State behaviour in cyberspace. These 11 voluntary and non-binding norms describe what a State should and should not do in the cyberspace.

This Checklist aims to provide actionable steps for all States to consider, including small States with limited capacities. States do not need to implement all steps in the checklist, but to consider the suggested steps in line with their respective national priorities and capacities. It is hoped that with these norms implemented, States will have a common understanding of what to expect from each other, thereby supporting international peace and security in cyberspace.

Using the Checklist

Each of the 11 norms and their actionable items will be displayed in the sample table format shown below.

Norm 13(x) Sample Norm Name *Full agreed text of norm*		
PILLARS	**VOLUNTARY STEPS TO BE CONSIDERED**	**SUGGESTED CAPACITY-BUILDING ACTIVITIES**
Pillar name	Detailed and actionable items on how the relevant government agencies can consider implementing the norm.	Possible capacity-building activities States can consider doing to meet the norm.

Within each norm, the items will be separated into five pillars: policy, operational, technical, legal, and diplomacy. This is to provide greater clarity on how different State agencies can contribute to these cyber norms. Meaningful implementation of the 11 cyber norms requires the involvement of multiple stakeholders and a whole-of-government approach. States may wish to consider setting up an inter-agency process to coordinate these discussions. The following gives more details of each pillar:

PILLAR NAME	SUGGESTED STATE AGENCIES TO REVIEW THE PILLAR	DESCRIPTION OF THE PILLAR
Policy	• Policy divisions in agencies in charge of cybersecurity	Suggests steps to take to set the direction and expectations a State has in mind for the norms.
Operational	• IT divisions in agencies in charge of cybersecurity • National CERTs/CSIRTs	Suggests steps to take that concerns day-to-day cyber-related State activities as well as cyber incident response.
Technical	• Technical divisions in agencies in charge of cybersecurity • IT divisions in agencies in charge of cybersecurity	Suggests steps to take to ensure that State's IT infrastructure, capability developments, and technical standards work towards fulfilling the norm.
Legal	• Law/justice/judicial ministry • Home affairs/law enforcement ministry • Legal divisions in agencies in charge of cybersecurity • Enforcement divisions in agencies in charge of cybersecurity	Suggests steps to take that concerns cyber-related legislation and law enforcement.
Diplomacy	• Foreign ministry • Policy divisions in agencies in charge of cybersecurity	Suggests steps to take that concern a State's international and foreign bilateral and multilateral interactions with other States.

Norm 13 (a)

Inter-State Cooperation on Cybersecurity *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*		
PILLARS	**STEPS TO BE TAKEN**	**SUGGESTED CAPACITY-BUILDING ACTIVITIES**

POLICY	1. Develop a national position on what constitutes harmful ICT practices.
	2. Establish the State's stance on inter-State interactions on cybersecurity matters.
	3. Identify States who are keen to cooperate on cybersecurity matters and determine ways in which the State can cooperate with other States.
	  a. This could be based on existing alliances or interests with other States.
	4. Develop an International Cooperation Strategy to guide the State's cooperation with other States on cybersecurity matters. The Strategy should outline:
	  a. An assessment of relevant trends in cybersecurity challenges faced by the international community.
	  b. The objectives and principles of interstate cooperation on cybersecurity.
	  c. How the various modalities of cooperation with other States (e.g., MOUs, agreements, dialogues etc.) can achieve these objectives and principles.
	5. Conduct periodic reviews of the Strategy to ensure that it is relevant and applicable to the evolving geopolitical and cybersecurity landscapes.
	6. Ensure that new and updated policies and frameworks are appropriately disseminated to the relevant parties.
	7. Seek whole-of-government support for the Strategy.
	8. Foreign policy that recognizes cybersecurity as one of the priorities.[2]
		• Regional/international projects and activities that seeks to build understanding and capacities for cybersecurity policy-making.
		• Exchanges with other States and international organizations to learn about their policies on interstate cooperation.
		• Basic cybersecurity knowledge for policy experts and practitioners.[1]

[1] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 17.

[2] Ibid.

OPERATIONAL	**1.** Establish/appoint a national CERT/CSIRT to respond to ICT incidents. **2.** Take measures at the national level to strengthen the functions of existing regional CERT/CSIRT. **3.** Work with other States' national CERTs/CSIRTs to strengthen incident response capabilities. **a.** CERTs/CSIRTs to work with could be based on existing national policies, MOUs, or States that are of interest to work with. **4.** Determine a mode of communication to facilitate information sharing between national CERTs/CSIRTs. **5.** Develop standard operating procedures and codes of conduct for communication with other States. **6.** Conduct simulation exercises with other States to strengthen cybersecurity cooperation and capabilities. **7.** Consider memberships to other regional and international CERT/CSIRT networks. **8.** Coordinate with other relevant local government agencies to develop and implement mechanisms to aid in inter-State communications. **9.** Consider cooperative and dialogue arrangements with the private sector, academia, civil society and the technical community.[3]	• CERT/CSIRT capacity-building programmes. • Incident response training courses. • Regional/international CERT/CSIRT drills and exercises. • Exchanges with other States and international organizations to learn about their best practices on inter-State cooperation.
TECHNICAL	**1.** Determine the equipment needed to form the infrastructure needed to facilitate information exchanges with other States. **2.** Design and implement the infrastructure based on cybersecurity principles and requirements specified in international standards and best practices. **3.** Conduct training for personnel that need to use and maintain the infrastructure. **4.** Conduct regular maintenance on the infrastructure. **5.** Encourage the development of cybersecurity capabilities, including: **a.** Capabilities to ensure cybersecurity endpoint protection (antivirus or automatic updates/patches for digital products to mitigate security bugs and vulnerabilities).[4]	• Conferences or trade exhibitions to keep updated on latest technological offerings. • Working with the private sector to implement the required infrastructure, hardware, and software.

[3] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 18; GGE. 2021. Final Substantive Report, para. 4.

[4] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 19.

	b. Technical capability to prevent, detect or disrupt malicious ICT acts.[5] **c.** Technical solutions to protect communications (e.g., encryption).[6]	
LEGAL	**1.** Train government officers with legal/judicial responsibilities to be versed in the legal aspects of cyber. **2.** Provide legal counsel to relevant agencies and ministries seeking interstate cooperation in cyber to ensure that agreements are drafted in accordance with local and international laws.	• Courses on the application of local and international laws in cyberspace. • Participation in regional and international forums and dialogues on cyber laws.
DIPLOMACY	**1.** Participate in relevant regional and international dialogues and forums, including at the United Nations. Activities could include: **a.** Exchanging best practices on cybersecurity with other States. **b.** Discussing efforts to implement the agreed norms of responsible State behaviour in cyberspace, as well as discussing possible additional norms of responsible State behaviour. **2.** Establish bilateral/multilateral relationships with other States for collaboration. **3.** Voluntarily share national and regional experiences on the implementation of norms, such as through the ASEAN regional action plan for norms implementation. **4.** Point of Contact (PoC) at the diplomatic and technical level.[7]	• International cybersecurity forums and dialogues to exchange information/ ideas and advance efforts to implement the agreed norms of responsible State behaviour as well as discuss possible additional norms of responsible State behaviour • Regular bilateral/multilateral dialogues with States.

[5] Ibid.

[6] Ibid.

[7] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 18.

Norm 13 (b)

Consider All Relevant Information *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*		
PILLARS	**STEPS TO BE TAKEN**	**SUGGESTED CAPACITY-BUILDING ACTIVITIES**
POLICY	1. Outline expectations of the State's department in charge of cybersecurity when handling an ICT incident. 2. Establish a whole-of-government policy to enable the government to collect and consider all relevant information when responding to national cyber incidents. 3. Establish an Attribution Framework that guides the government on the decision-making process of attributing an ICT incident. Some guiding questions could be: **a.** Is the incident attributable? **b.** Is it in the State's interest to make a formal attribution? **c.** What are the types of attribution mechanisms available? **d.** Which stakeholders should be involved? 4. Conduct periodic reviews of frameworks to ensure that they are relevant and applicable to the evolving geopolitical and cybersecurity landscapes. 5. Ensure that new and updated frameworks are appropriately disseminated to the relevant parties.	• Collaborating with other States and international organizations to learn about how they carry out ICT incident response and investigations. • Discussions and exchanges on the types of attribution tools and mechanisms available to States.
OPERATIONAL	1. Create/appoint a national CERT/CSIRT to respond to ICT incidents. 2. Develop incident reporting templates for structured reporting of a suspected ICT incident within the State. 3. Create playbooks for responding to reported ICT incidents. The playbooks may cover the following: **a.** The incident's technical attributes; **b.** Its scope, scale, and impact; **c.** The wider context, including the incident's bearing on international peace and security; **d.** The results of consultations between the States concerned; [8]	• CERT/CSIRT capacity building programmes. • Incident response training courses. • National/regional/international CERT/CSIRT drills and table-top exercises. • Collaborating with other stakeholders to learn about how they carry out ICT incident response and investigations.

[8] See OEWG. 2024. Final Substantive Report, Annex A, Norm B (2).

OPERATIONAL	**e.** How to respond to a variety of possible national ICT incidents; and **f.** The relevant national leadership teams to report findings to. **4.** Reference and, wherever possible, contribute to cybersecurity information repositories to obtain information about threats related to the ICT incident. **5.** Cooperate with other States' CERTs/CSIRTs and CERT/CSIRT networks to allow for transnational information exchange to aid with ICT incident investigations (especially for transnational ICT incidents). **6.** Establish a dedicated government agency that will be responsible for the coordination, assessment, and decision-making in the event of cyber incidents. **a.** Avoid overlaps in responsibilities to prevent potential conflicts of interest. **7.** Form whole-of-government communication channels to allow for efficient consultations. **8.** Conduct regular training and simulation exercises for personnel involved in cyber incident response to hone their skills and for validation of communication channels.	
TECHNICAL	**1.** Determine the equipment needed to form the infrastructure to facilitate effective cyber incident investigations. **2.** Design and implement the infrastructure based on advanced technologies and requirements specified in international standards and best practices. **3.** Conduct training for personnel that need to use and maintain the infrastructure. **4.** Conduct regular maintenance on the infrastructure.	• Develop technical and forensic capabilities to investigate and determine the source of malicious activity.[9] • Working with the private sector to implement the required infrastructure, hardware, and software.
LEGAL	**1.** Train government officers with legal/judicial responsibilities to be versed in the legal aspects of cyber. **2.** Consider if legislation needs to be introduced to prohibit malicious ICT acts within the State. **3.** Empower and train local law enforcement to apprehend threat actors who are involved in ICT incidents and physically located within the State's jurisdiction. **4.** Consider if legislation needs to be introduced to authorize respective government agencies to access all relevant information relating to the cyber incident.	• Courses on application of local and international laws in cyberspace. • Courses that prepare States to implement cyber-related legal frameworks into their own legislations. • Regional and international forums and dialogues on cyber laws. • Law enforcement training.

[9] Ibid., 21.

LEGAL	**5.** Participate in regional and international forums to discuss about international law pertaining to ICT and cyberspace. **6.** Consider decision frameworks on how to respond to malicious ICT activity attributable to another State that are in accordance with a State's obligations under the Charter of the United Nations and other international law, including those relating to the settlement of disputes by peaceful means and internationally wrongful acts.[10] **7.** Provide legal counsel to relevant agencies and ministries in the government to ensure that policies and procedures are in accordance with local and international laws.	
DIPLOMACY	**1.** Establish diplomatic channels with other States to allow for diplomatic communications during a cyber incident to exchange information and seek assistance. **2.** Conduct regular bilateral/multilateral dialogues with States.	• International cybersecurity forums and dialogues to exchange information/ideas and agree on norms.

[10] See OEWG. 2024. Final Substantive Report, Annex A, Norm B (3).

Norm 13 (c)

Prevent Misuse of ICTs in One's Territory *States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs*		
PILLARS	**STEPS TO BE TAKEN**	**SUGGESTED CAPACITY-BUILDING ACTIVITIES**
POLICY	**1.** Cybersecurity strategy or policy setting out the provisions to take action (e.g., detecting and interrupting) in case of a malicious ICT incident.[11] **2.** Establish policies on the State's position on the misuse of ICT systems within its territory. **3.** Develop policies to prevent the misuse of ICT systems within one's territory. **a.** The State is encouraged to adopt a whole-of-government as well as a multi-stakeholder approach in the prevention of misuse of ICT systems in one's territory. **b.** The State is also encouraged to cooperate with other States to prevent the misuse of ICTs in one's territory. **4.** Consider working through relevant government agencies to establish a culture of good cyber hygiene among the citizens, businesses, and other organizations. **5.** Conduct periodic reviews of policies to ensure that they are relevant and applicable to the evolving geopolitical and cybersecurity landscapes. **6.** Ensure that new and updated policies are appropriately disseminated to the relevant parties.	• Collaborating with other States and international organizations to learn about how they manage and prevent ICT misuse.
OPERATIONAL	**1.** Create/appoint a national CERT/CSIRT to respond to ICT incidents. **2.** Develop incident reporting templates for structured reporting of a suspected ICT incident within the State. **3.** Create playbooks for national CERT/CSIRT to respond, and resolve malicious ICT operations. **4.** Establish communication channels with other States to allow them to reach out for assistance or to notify on cases of misuse of ICT systems at the operational level, e.g., through national CERTs/CSIRTs and CERT/CSIRT networks. **a.** Where possible, States should consider extending this to more States or international law enforcement organizations.	• CERT/CSIRT capacity-building programmes. • Incident response training courses. • Regional/international CERT/CSIRT drills and exercises. • Collaborating with other States and international organizations to learn about how they manage and prevent ICT misuse.

[11] Ibid.

OPERATIONAL	**b.** Where possible States should consider extending this to relevant stakeholders at national and regional levels. **5.** Conduct training for personnel to be competent in detecting malicious cyber activities and enforcing the law on perpetrators. **6.** Set up active threat monitoring to track and stop ICT misuse as fast as possible. **7.** Establish a dedicated government agency that specializes in countering and responding to malicious cyber activities. This could be a standalone agency or a branch of the State's law enforcement force. **8.** Devise regional mechanisms to enable real-time collaboration during an active ICT incident. **9.** In the case of an ICT incident, the following steps could be undertaken: **a.** An affected State should notify the State from which the activity is emanating; **b.** The notified State should acknowledge receipt of the notification to facilitate cooperation and clarification. Acknowledging the receipt of this notice does not indicate concurrence with the information contained therein; **c.** The notified State should make every reasonable effort to assist in establishing whether an internationally wrongful act has been committed. [12] **10.** Consider developing separate communication guidelines if an incident involves more than two regional States.	
TECHNICAL	**1.** Determine the equipment needed to form the infrastructure needed by the government agency/branch specializing in countering and responding to malicious cyber activities to be able to carry out its operations. **2.** Design and implement the infrastructure based on cybersecurity principles and requirements specified in international standards and best practices. **3.** Conduct training for personnel that need to use and maintain the infrastructure. **4.** Conduct regular maintenance on the infrastructure. **5.** Perform incident response to detect, analyse, and report incidents. **6.** Conduct research and development to improve threat monitoring and incident response systems.	• Conferences or trade exhibitions to keep updated on the latest technological offerings. • Working with the private sector to implement the required infrastructure, hardware, and software.

[12] See OEWG. 2024. Final Substantive Report, Annex A, Norm C (3).

TECHNICAL	**7.** Access to cybersecurity expertise, either internal or external, to identify and disrupt malicious ICT acts emanating from their territory (e.g., network security skills).[13] **8.** Consider implementing the processes for interagency collaborations within the Government and public–private partnerships.	
LEGAL	**1.** Train government officers with legal/judicial responsibilities to be versed in the legal aspects of cyber, in particular on the concept of due diligence. **2.** Empower and train local law enforcement to apprehend threat actors who are involved in ICT incidents and physically located within the State's jurisdiction. **3.** Provide legal counsel to relevant agencies and ministries in the government to ensure that policies and procedures are in accordance with local and international laws.	• Courses on the application of local and international laws in cyberspace. • Courses that prepare States to implement cyber-related legal frameworks into their own legislations. • Regional and international forums and dialogues on cyber laws. • Law enforcement training.
DIPLOMACY	**1.** Participate in dialogues to collaborate with other States on norms on responsible State behaviour in cyberspace. **2.** Participate in relevant regional and international forums to keep up to date on the latest threats and to exchange information with foreign counterparts.	• International cybersecurity forums and dialogues to exchange information/ideas on norms. • Regular bilateral/multilateral dialogues with States.

[13] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 22.

Norm 13 (d)

Cooperate to Stop Cybercrime & Terrorism *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*		
PILLARS	**STEPS TO BE TAKEN**	**SUGGESTED CAPACITY-BUILDING ACTIVITIES**
POLICY	**1.** Establish the State's position on inter-State cooperation on cybercrime and terrorism matters. **2.** Assess if the State's existing memberships in regional and international groups (if any) are applicable in cooperating to stop cybercrime and terrorism. **3.** 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.[14] **4.** Identify States that are keen to cooperate on cybercrime and terrorism matters. **5.** Determine ways in which the State can cooperate with other States identified in Step 3 to achieve this norm. **6.** Develop an International Cooperation Strategy to guide the State's cooperation with other States on cybercrime and terrorism matters. The Strategy may include: **a.** An assessment of relevant trends in cybercrime and terrorism. **b.** A statement of the objectives and principles of international cooperation in this regard. **c.** A statement of how the various modalities of international cooperation can achieve these objectives and principles. **d.** A statement of plans for building the State's national capabilities to allow it to work with foreign counterparts and organizations. **7.** Conduct periodic reviews of the strategy to ensure that they are relevant and applicable to the current geopolitical and cybersecurity landscapes. **8.** Ensure that the new and updated strategy is appropriately disseminated to the relevant parties.	• Reading State and international organizations' papers and case studies that give insights on how they combat cybercrime and terrorism in their respective jurisdictions.

[14] Ibid.

OPERATIONAL	**1.** Establish/appoint a national CERT/CSIRT or dedicated government agency to assist the national /foreign law enforcement agencies with cybercrime and terrorism investigations. **2.** Strengthen existing standard operating procedures and guidelines on interacting with foreign counterparts and international organizations handling cybercrime and terrorism. **3.** Train relevant personnel to be competent in working with foreign counterparts and international organizations to combat cybercrime and terrorism. **4.** Conduct regular exercises to ensure preparedness to respond to cyber threats. This could be in collaboration with foreign counterparts and international organizations. **5.** Set up communication mechanisms that will allow the agency/branch to communicate with foreign and local counterparts and international organizations (e.g., INTERPOL) at an operational level.	• CERT/CSIRT capacity-building programmes. • Incident response training courses. • National /regional/inter-national CERT/CSIRT drills and exercises. • Reading State and international organizations' papers and case studies that give insights on how they combat cybercrime and terrorism in their respective jurisdictions.
TECHNICAL	**1.** Determine the equipment needed to form the infrastructure to engage in international cooperation and combat cybercrime and terrorism. **2.** Design and implement the infrastructure based on cybersecurity principles and requirements specified in international standards and best practices. **3.** Identify and encourage relevant government agencies to take internationally recognized cybercrime enforcement certifications to ensure a certain standard of capabilities in combating cybercrime and terrorism.	• Conferences or trade exhibitions to keep updated on the latest technological offerings. • Working with the private sector to implement the required infrastructure, hardware, and software.
LEGAL	**1.** Train government officers with legal/judicial responsibilities to be versed in the legal aspects of cyber. **2.** Study the feasibility of introducing legislation that prohibits the misuse of ICT systems within the State's territory. **3.** Study the feasibility of creating a legal framework that authorizes the government to criminalize errant usages of ICT systems. **4.** Introduce legislation on the criminal or terrorist use of ICT to deter such activities. **5.** Provide training to local law enforcement agencies to be able to apprehend and stop cybercrime and terrorism.	• Courses on the application of local and international laws in cyberspace. • Courses that prepare States to implement cyber-related legal frameworks into their own legislations. • Regional and international forums and dialogues on cyber laws. • Law enforcement training. • Member States to have experts who can handle digital evidence at the technical and legal levels (e.g., training on writing mutual legal assistance requests). [15]

[15] Ibid., 25.

LEGAL	**6.** Participate in international forums to discuss the application and development of international law with respect to cybercrime and terrorism. **7.** Consider working with other States or international law enforcement organizations to combat transnational cybercrime and terrorism. **8.** Provide legal counsel to relevant agencies and ministries in the government to ensure that policies and procedures are in accordance with local and international laws. **9.** Set up proper protocols and procedures that consent to use digital evidence in court.[16] **10.** 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 terrorist use of ICTs.[17]	
DIPLOMACY	**1.** Participate in relevant regional and international forums to keep up to date on the latest cybercrimes and to exchange information with foreign counterparts and international organizations. **2.** Participate in international forums to discuss the application and development of international law with respect to cybercrime and terrorism. **3.** Participate in dialogues to collaborate with other States to agree on norms on responsible State behaviour in cyberspace.	• International cybersecurity forums and dialogues to exchange information/ideas on norms. • Regular bilateral/multilateral dialogues with States.

[16] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 24

[17] Ibid., 25.

Norm 13 (e)

Respect Human Rights & Privacy *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*		
PILLARS	**STEPS TO BE TAKEN**	**SUGGESTED CAPACITY-BUILDING ACTIVITIES**
POLICY	1. Establish the State's position on human rights in cyberspace which should take into account the resolutions adopted at the United Nations. 2. Where applicable, review the State's existing policies to evaluate if the same human rights that apply offline could be extended online. 3. Ensure disadvantaged groups in the country enjoy equal opportunities and rights regarding ICT. 4. Conduct periodic reviews of the policies and strategies to ensure that they are relevant and applicable to the evolving geopolitical and cybersecurity landscapes. 5. Ensure that new and updated policies and strategies are appropriately disseminated to the relevant parties.	• Collaborating with other States and international organizations to learn about how they observe and implement cyber policies that respect human rights and privacy.
OPERATIONAL	1. Educate the public about their individual rights (e.g., data privacy rights) on the Internet.	• Courses about data protection and privacy in cyber. • Collaborating with other States and international organizations to learn about how they observe and implement cyber policies that respect human rights and privacy.
TECHNICAL	1. Identify the infrastructure and technologies required to ensure that the State's ICT infrastructure is capable of protecting user's human and privacy rights (e.g., cell networks supporting cryptography for the privacy of communications). 2. Design and implement the infrastructure based on cybersecurity principles and requirements specified in international standards and best practices.	• Conferences or trade exhibitions to keep updated on the latest technological offerings. • Working with the private sector to implement the required infrastructure, hardware, and software. • Working with international standards and certification organizations to learn more about the standards and certifications available.

TECHNICAL	**3.** Adopt existing international/regional standards and/or develop national standards that businesses and organizations can use to guide their data management practices. **a.** These standards and certifications could be based on internationally recognized equivalents. **b.** The government plays an important role to promote and support the implementation of these international standards in local businesses.	
LEGAL	**1.** Train government officers with legal/judicial responsibilities to be versed in the legal aspects of human rights and cyber. **2.** Participate in international forums and dialogues to promote and develop understandings on (international) laws on human rights and privacy in the context of cyberspace. **3.** Establish State's position on how existing legislations on human rights and privacy is applicable to the cyber context. **4.** Study the feasibility of legislation that will protect user's human rights and privacy in cyberspace. **5.** Provide training to law enforcement for them to assist in apprehending individuals or entities who violate human rights laws. **6.** Provide legal counsel to relevant agencies and ministries in the government to ensure that policies and procedures are in accordance with local and international laws.	• Courses on laws pertaining to human rights and privacy. • Courses that prepare States to implement cyber-related legal frameworks into their own legislations. • Regional and international forums and dialogues on cyber laws. • Law enforcement training. • Public officials (including those working in law enforcement agencies) must have knowledge of human rights in the digital domain as well as of how to implement international instruments (e.g., mutual legal assistance requests) in a way that is consistent with human rights.[18]
DIPLOMACY	**1.** Collaborate with other States to promote principles of human rights and privacy in cyberspace including through participation in relevant dialogues and forums. **2.** Participate in international discussions of the protection of human rights in cyberspace, including at the United Nations.	• International cybersecurity forums and dialogues to exchange information/ideas and agree on norms. • Regular bilateral/multilateral dialogues with States.

[18] Ibid., 27.

Norm 13 (f)

Do Not Damage Critical Infrastructure *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*		
PILLARS	**STEPS TO BE TAKEN**	**SUGGESTED CAPACITY-BUILDING ACTIVITIES**
POLICY	**1.** Develop and make publicly available a national position on how international law applies to the use of ICT by States.[19] **2.** Establish a policy on the government's position on not damaging critical infrastructures (CIs) and critical information infrastructures (CIIs). **a.** The policy should also adopt a multi-stakeholder approach to encourage multiple parties, including the private sector, academia, and public, to support a commitment to not damaging CIs and CIIs. **3.** Determine which infrastructure or sectors to deem critical within your State's jurisdiction, in accordance with national priorities and methods of categorization of critical infrastructure.[20] **4.** National interpretations of the term "knowingly support", their classifications of ICT incidents in terms of scale, seriousness (including with reference to what constitutes 'damage' and 'impairment'), and their understanding of what constitutes, considering their national context, "critical infrastructure".[21] **5.** Conduct periodic reviews of the policy to ensure that it is relevant and applicable to the evolving geopolitical and cybersecurity landscapes. **6.** Ensure that new and updated policy is appropriately disseminated to the relevant parties.	• Reading State and international organizations' papers that outlines their positions on not damaging CIs and CIIs. • Reading of States' strategy papers which identify the CI or CII sectors of that State.

[19] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 28.

[20] See OEWG. 2024. Final Substantive Report, Annex A, Norm F (1).

[21] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 28

OPERATIONAL	**1.** Coordinate with the military, defence ministry, national CERT/CSIRT, and other relevant government agencies to establish a common ground and understanding regarding the protection of CIs and CIIs. It should be agreed that organizations with offensive capabilities should not conduct or knowingly support ICT activity that damages CIs and CIIs contrary to State's obligations under international law. **2.** Establish a dedicated office within the government that will fulfil the abovementioned Steps. **3.** Set up independent, effective domestic or regional oversight mechanisms (judiciary, administrative, parliamentary) capable of ensuring transparency on Member States' conduct (e.g., parliamentary committee).[22]	• Reading of States' strategy papers that identify the CI or CII sectors of that State. • Exchanging information with other States about CI and CII protection measures. • Regional/international CERT/CSIRT drills and exercises.
TECHNICAL	**1.** Explore the feasibility of implementing safeguards and detection of cyberattacks emanating from the State.	• Conferences or trade exhibitions to keep updated on the latest technological offerings. • Working with the private sector to implement the required infrastructure, hardware, and software. • Working with international standards and certification organizations to learn more about the standards and certifications available.
LEGAL	**1.** Train government officers with legal/judicial responsibilities to be versed in the legal aspects of cyber. **a.** If necessary, recruit legal experts from the respective critical infrastructure (CI) and critical information infrastructure (CII) sectors to obtain their subject matter expertise. **2.** Encourage State leaders to, on behalf of the State, publicly declare their commitment to respecting and adhering to international laws governing cyberspace. **3.** Provide legal counsel to relevant agencies and ministries in the government to ensure that policies and procedures are in accordance with local and international laws.	• Courses on the application of local and international laws in cyberspace. • Regional and international forums and dialogues on cyber laws. • 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).[23]

[22] Ibid.

[23] Ibid.

DIPLOMACY	**1.** Participate in regional and international dialogues with other States to build confidence and common ground about the importance of critical infrastructures (CIs) and critical information infrastructures (CIIs) for essential services. **2.** Participate in regional and international dialogues with other States to agree not to use offensive capabilities on CIs and CIIs. **3.** Participate in regional and international dialogues and forums that discusses about cybersecurity issues and other relevant issues. **4.** Seek and establish bilateral and/or multilateral agreements with other States to build common understanding and cooperation and reduce the risk of escalation and conflict.	• Reading of States' strategy papers that identify the CI or CII sectors of that State. • International cybersecurity forums and dialogues to exchange information/ideas on norms. • Regular bilateral/multilateral dialogues with States.

Norm 13 (g)

Protection of Critical Infrastructure *States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions*		
PILLARS	**STEPS TO BE TAKEN**	**SUGGESTED CAPACITY-BUILDING ACTIVITIES**
POLICY	**1.** Develop a framework for the identification of critical infrastructures (CIs) and critical information infrastructures (CIIs). **2.** Adopt a policy framework suitable for the protection of critical infrastructure and the classifications of ICT incidents in terms of scale and seriousness specific to their critical infrastructure (e.g., establishing regulations on their construction, including minimum security standards, reporting mechanisms, and audits).[24] **3.** Have emergency warning networks regarding ICT vulnerabilities, threats, and incidents.[25] **4.** Develop a framework for the protection of CIs and CIIs, which may include: **a.** Regulatory levers to protect CIs and CIIs. **b.** Non-regulatory levers to protect CIs and CIIs. **5.** Encourage cross-border cooperation with relevant critical infrastructure owners and operators to enhance the ICT security measures accorded to such infrastructure and strengthen existing or develop complementary processes and procedures to detect and mitigate ICT incidents affecting such infrastructure.[26] **6.** Conduct periodic reviews of the frameworks to ensure that they are relevant and applicable to the evolving geopolitical and cybersecurity landscapes. **7.** Ensure that any new and updated framework is appropriately disseminated to the relevant parties.	• Collaborating with other States and international organizations to learn about how they protect their own CIs and CIIs. • Raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them.[27]

[24] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 29.

[25] See OEWG. 2024. Final Substantive Report, Annex A, Norm G (1).

[26] Ibid.

[27] Ibid.

OPERATIONAL	**1.** Appoint relevant agencies or divisions to oversee the implementation of critical infrastructure (CI) and critical information infrastructure (CII) protection mechanisms. **2.** Establish sectoral CERT/CSIRT to respond to ICT incidents for CIs and CIIs. **3.** Set up cross-border cooperation and exchanges with relevant stakeholders (e.g., operators and owners).[28] **4.** Establish cooperation mechanisms between relevant domestic stakeholders (interagency committees, multi-stakeholder platforms) including public–private partnerships with critical infrastructure owners, operators or managers.[29] **5.** Assign points of contact (PoC)/sector leads for each CI or CII. **6.** Develop a code of practice/conduct for sector leads to refer to during incidents. **7.** Create an emergency contact mechanism for CI and CII owners to contact the national CERT/CSIRT and/or relevant government agency when they are under a cyberattack. **8.** Vendors should ensure the safety and security of ICT products throughout their life cycle.[30] **9.** Classify ICT incidents in terms of their scale and seriousness.[31] **10.** Conduct/implement mandatory cyber risk assessments and audits. **11.** Design mechanisms for information sharing with and among CI and CII sectors and train sector leads. **a.** To build capacity during incidents. **b.** To enhance detection, analysis, and response capabilities. **12.** Develop plans for responding to cyber crises and exercise these plans at a national and sectoral level (e.g., table-top exercises).	• CERT/CSIRT capacity-building programmes. • Incident response training courses. • Regional/international CERT/CSIRT drills and exercises. • Collaborating with other States and international organizations to learn about how they protect their own CIs and CIIs.

[28] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 30.

[29] Ibid.

[30] See OEWG. 2024. Final Substantive Report, Annex A, Norm G (1).

[31] See OEWG. 2024. Final Substantive Report, Annex A, Norm G (2).

OPERATIONAL	**13.** Create a dedicated multi-agency and multi-stakeholder consultation mechanism to protect CIs and CIIs. **a.** To take inventory of the current state of CIs and CIIs (recurring, depending on what the State deems important). **b.** To evaluate the risk assessment of each CI and CII (recurring, depending on the situation). **14.** Establish a threat monitoring centre to monitor for attacks on CIs and CIIs. **15.** States hosting regional infrastructure should encourage cross-border cooperation with relevant infrastructure owners and operators to enhance the ICT security measures accorded to such infrastructure and strengthen existing or develop complementary processes and procedures to detect and mitigate ICT incidents affecting such infrastructure.[32]	
TECHNICAL	**1.** Identify the infrastructure and technologies needed to implement safeguards and protection mechanisms for critical infrastructures (CIs) and critical information infrastructure (CIIs). **a.** Wherever possible, liaise with personnel from the respective CIs and CIIs to understand their unique infrastructure and requirements. **2.** Design and implement the infrastructure based on cybersecurity principles and requirements specified in international standards and best practices. **3.** Adopt international certifications and/or develop national standards for CIs and CIIs to adhere to for them to be able to establish a minimum standard of cybersecurity to defend against cyberattacks. **4.** Technical capability to prevent, detect or disrupt malicious ICT acts targeting critical infrastructure. Including but not limited to, threat intelligence platforms, early warning systems, tools for vulnerabilities scanning and secured ICT perimeters.[33]	• Conferences or trade exhibitions to keep updated on the latest technological offerings. • Working with the private sector to implement the required infrastructure, hardware, and software. • Working with international standards and certification organizations to learn more about the standards and certifications available.

[32] GGE. 2021. Final Substantive Report, para. 49.

[33] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 30.

LEGAL	**1.** Train government officers with legal/judicial responsibilities to be versed in the legal aspects of cyber. **a.** If necessary, recruit legal experts from the respective critical. infrastructure sectors to obtain their subject matter expertise. **2.** Study the feasibility of drafting and introducing legislation – e.g., a Cybersecurity Act to prescribe minimum standards for the security of CIs and CIIs. **3.** Train law enforcement personnel to be prepared to respond to ICT incidents. **4.** Provide legal counsel to relevant agencies and ministries in the government to ensure that policies and procedures are in accordance with local and international laws. **5.** Establish regulations on information exchange among the public and private sectors involved.[34]	• Courses on the application of local and international laws in cyberspace. • Courses that prepare States to implement cyber-related legal frameworks into their own legislations. • Regional and international forums and dialogues on cyber laws. • Law enforcement training.
DIPLOMACY	**1.** Participate in regional and international dialogues and forums that discuss about cybersecurity issues and other relevant topics. **2.** Set of skills for diplomats to engage with their counterparts on the specific topic of critical infrastructure particularly if the infrastructure is transnational.[35] **3.** Seek opportunities to engage with other States to cooperate in cybersecurity to strengthen cybersecurity capabilities and defence. **a.** This can be through joint bilateral/multilateral exercises or mutual agreements.	• International cybersecurity forums and dialogues to exchange information/ideas on norms. • Regular bilateral/multilateral dialogues with States.

[34] Ibid., 29.

[35] Ibid.

Norm 13 (h)

Respond to Requests for Assistance *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*		
PILLARS	**STEPS TO BE TAKEN**	**SUGGESTED CAPACITY-BUILDING ACTIVITIES**
POLICY	1. Establish a framework for assessing areas in which the State is prepared and able to provide assistance. 2. Ensure that data availability policies take into account the need to protect critical information infrastructures (CII).[36] 3. Establish a policy that outlines the State's position on responding to requests from other States and international organizations for assistance. a. This helps other States and organizations to have some form of assurance that the State is willing to assist and cooperate in tackling cybersecurity issues. 4. Conduct periodic reviews of the policies and frameworks to ensure that they are relevant and applicable to the evolving geopolitical and cybersecurity landscapes. 5. Ensure that new and updated policies and frameworks are appropriately disseminated to the relevant parties.	• Collaborating with other States and international organizations to learn about how they carry out ICT incident response and investigations and share best practices.
OPERATIONAL	1. Appoint relevant agencies or divisions to oversee the operational processes when responding to foreign States' requests. 2. Nominate the national CERT/CSIRT as the point of contact for requests for assistance. 3. Join regional and global point of contact directories to strengthen communication channels with other States and international organizations and be kept abreast of the concerns in cybersecurity/cybercrimes within the region and internationally. a. This can also include the national CERT/CSIRT joining international and regional CERT/CSIRT networks.	• CERT/CSIRT capacity-building programmes. • Incident response training courses. • Regional/international CERT/CSIRT drills and exercises. • Collaborating with other States and international organizations to learn about best practices to request for assistance and respond to one. • Personnel receiving or sending requests for assistance should clearly understand how to address and manage a request for assistance.[37]

[36] See OEWG. 2024. Final Substantive Report, Annex A, Norm H (6).

[37] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 32.

OPERATIONAL	**4.** Create a mechanism to help standardize and facilitate the receiving, processing, evaluation, and responding to requests of assistance from other States.[38] **a.** Seek the services of the private sector to assist in responding to requests for assistance where appropriate.[39] **b.** The receiving State should acknowledge receipt of the request and, if assistance is possible, an indication of the time frame, nature, scope and terms of the assistance that could be provided.[40] **5.** Establish a dedicated office within the government that will manage communications from other States and international organizations on matters related to cybersecurity. **a.** Ideally, this office should also have links with other local government agencies as well as key stakeholders (e.g., CI and CII owners) to be able to facilitate efficient communications in the event of a cyber incident. **6.** Where necessary, the national CERT/CSIRT should work with other incident response teams within the State such as security operations centres of critical infrastructures (CIs) and critical information infrastructures (CIIs) to respond to requests for assistance.	• Participate in simulation exercises for CERTs/CSIRTs and other relevant parties to ensure that the State is ready to handle requests for assistance. This can also extend to regional or international exercises, which can help to strengthen the State's ability to work with other States to render assistance.
TECHNICAL	**1.** Determine the equipment needed to form the infrastructure needed to facilitate communications with other States. **2.** Design and implement the infrastructure based on cybersecurity principles and requirements specified in international standards and best practices. **3.** Provide support to, at minimum, government agencies and critical infrastructure (CI) and critical information infrastructure (CII) owners, to be certified by internationally recognized standards and certifications related to cybersecurity management and cyber incident response.	• Conferences or trade exhibitions to keep updated on the latest technological offerings. • Working with the private sector to implement the required infrastructure, hardware, and software. • Working with international standards and certification organizations to learn more about the standards and certifications available.

[38] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 31.

[39] See OEWG. 2024. Final Substantive Report, Annex A, Norm H (3).

[40] GGE. 2021. Final Substantive Report, para. 54.

LEGAL	**1.** Train government officers with legal/judicial responsibilities to be versed in the legal aspects of cyber. **2.** Study the feasibility of introducing or strengthening existing legislation to allow the government to respond to support requests for assistance from other States. **3.** Train local law enforcement to be prepared to assist in assistance requests from other States. **4.** Provide legal counsel to relevant agencies and ministries in the government to ensure that policies and procedures are in accordance with local and international laws.	• Courses on the application of local and international laws in cyberspace. • Courses that prepare States to implement cyber-related legal frameworks into their own legislations. • Regional and international forums and dialogues on cyber laws.
DIPLOMACY	**1.** Participate in regional and international dialogues and forums that discuss about cybersecurity issues and other relevant topics. **a.** These are also opportunities for the State to publicly endorse and display its commitment to work with the international community to defend cyberspace. **2.** Seek opportunities to engage with other States and other stakeholders to cooperate in cybersecurity to strengthen cybersecurity capabilities and defence. **a.** This can be through exercises or mutual agreements. **3.** Where required to mitigate malicious ICT activity aimed at CI and CII, seek or offer assistance bilaterally or through regional or international arrangements, taking into account due regard for sovereignty.[41] **4.** Seek the services of the private sector to assist in responding to requests for assistance where appropriate.[42] **5.** Engage in cooperative mechanisms that define the means and mode of ICT crisis communications and of incident management and resolution, including through establishing at the regional-level common and transparent processes, procedures and templates.	• International cybersecurity forums and dialogues to exchange information/ideas on norms. • Regular bilateral/multilateral dialogues with States.

[41] See OEWG. 2024. Final Substantive Report, Annex A, Norm H (2).

[42] See OEWG. 2024. Final Substantive Report, Annex A, Norm H (3).

Norm 13 (i)

Ensure Supply Chain Security *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*		
PILLARS	**STEPS TO BE TAKEN**	**SUGGESTED CAPACITY-BUILDING ACTIVITIES**
POLICY	**1.** Identify the State's critical supply chains. **a.** As a start, the focus can be on supply chains that provide products and services to critical infrastructures (CIs) and critical information infrastructures (CIIs). **2.** Identify existing mechanisms that are in place to protect the security of the supply chains. If not, pass legislation prohibiting the introduction of harmful hidden functions and exploitation vulnerabilities in ICT products[43] to ensure greater software transparency at national, regional, and international levels. **3.** States should develop strategy to encourage the private sector and civil society to play an appropriate role to improve the security of and in the use of ICTs, including supply chain security for ICT products.[44] **4.** Develop a strategy for ensuring the security of supply chains. **a.** Due to the diversity and complexity of the ICT ecosystem, it is highly recommended to adopt a multi-stakeholder approach for the development of this strategy. **b.** Ensure the confidentiality, integrity and availability of the supply chains that provide products and services to CIs and CIIs. **c.** Establish measures to enhance the integrity of the supply chain, including by requiring ICT vendors to incorporate safety and security in the design, development and throughout the life cycle of ICT products. Consider establishing independent and impartial certification processes.	• Collaborating with other States and international unions to learn about best practices on governing the security by design of supply chains.

[43] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 33

[44] GGE. 2021. Final Substantive Report, para. 59.

POLICY	5. Adopt a cybersecurity 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.[45] 6. Conduct periodic reviews of the strategy to ensure that they are relevant and applicable to the evolving geopolitical and cybersecurity landscapes. 7. Ensure that any new and updated strategy is appropriately disseminated to the relevant parties.	
OPERATIONAL	1. Appoint relevant agencies or divisions to oversee the management of national supply chain security. 2. Engage with stakeholders such as industry partners and academia to understand cybersecurity's challenges and opportunities in supply chain security. 3. Work with stakeholders to identify opportunities or areas to strengthen the security posture of ICT supply chains and the overall ecosystem. 4. Establish international cooperation on recognizing ICT products and services that meet a certain standard of cybersecurity. 5. Establish a national CERT/CSIRT. 6. Train the national CERT/CSIRT to be ready to respond to supply chain attacks, especially those that affect the State's critical infrastructures (CIs) and critical information infrastructures (CIIs). 7. Establish a dedicated government office that will oversee the management of national supply chain security and fulfil the abovementioned steps. 8. Conduct regular audits on CI and CII owners to ensure their resilience and ability to minimize impact from cybersecurity incidents involving supply chains. 9. Establish a threat-hunting team to actively search for potential cybersecurity threats that could impact the security of ICT supply chains and the greater ecosystem. a. States can also engage big tech companies with their own threat-hunting teams to assist the government with threat monitoring.	• Training courses to build understanding about securing supply chains. • Training courses to train government personnel to be competent in conducting cyber risk assessments and audits for supply chain owners. • CERT/CSIRT capacity-building programmes. • Incident response training courses.

[45] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 33

OPERATIONAL	**10.** Strengthen partnership with the private sector to collaboratively enhance the security of and in the use of ICTs. Continue to encourage the private sector to play an appropriate role to improve the security of and in the use of ICTs, including supply chain security for ICT products, in accordance with the national laws and regulations of the States within which they operate.[46]	
TECHNICAL	**1.** Adopt international certification schemes or develop a national certification scheme for testing products and systems to be deemed as having met a certain standard of security. **a.** Ideally, this scheme should also be made in such a way that is easy for consumers to identify that a product or system has been tested and meets some cybersecurity standard. **b.** The certifications should be aligned with internationally recognized standards or schemes. **c.** The certification scheme could be mutually recognized internationally to maximize the benefits for manufacturers to have their products certified for export to various markets. **2.** Introduce a national certification scheme for organizations, including supply chain companies, to ensure that their cybersecurity standards are up to par with international standards. **3.** Introduce regional certification framework/mechanism to ensure greater software transparency among member states. **4.** Identify and, if necessary, implement infrastructure and/or technologies that can help the government protect supply chains (e.g., monitor for supply chain attacks).	• Conferences or trade exhibitions to keep updated on the latest technological offerings. • Working with the private sector to implement the required infrastructure, hardware, and software. • Working with international standards and certification organizations to learn more about the standards and certifications available.
LEGAL	**1.** Train government officers with legal/judicial responsibilities to be versed in the legal aspects of cyber. **a.** If necessary, recruit legal experts from the respective critical infrastructure (CI) and critical information infrastructure (CII) sectors to obtain their subject matter expertise. **2.** Study the feasibility to introduce legislation for CI and CII owners to be legally required to ensure that they have oversight and management of their supply chain partners.	• Courses on the application of local and international laws in cyberspace. • Courses that prepare States to implement cyber-related legal frameworks into their own legislations. • Regional and international forums and dialogues on cyber laws.

[46] See OEWG. 2024. Final Substantive Report, Annex A, Norm I (6).

LEGAL	**a.** This is to ensure that these owners take responsibility for holding their supply chain partners accountable. **3.** Study the feasibility to introduce legislation for supply chain companies who provide services to CI and CII owners to meet a certain level of security before they can provide services to CIs and CIIs. **4.** Provide legal counsel to relevant agencies and ministries in the government to ensure that policies and procedures are in accordance with local and international laws. **5.** Consider at the national level frameworks and mechanisms for supply chain risk management, consistent with a State's international obligations, taking into account a variety of factors, including the benefits and risks of new technologies.[47]	
DIPLOMACY	**1.** Participate in relevant regional and international forums to learn and exchange information about existing and emerging threats related to the ICT industry and its supply chains. **2.** Establish bilateral and/or multilateral cooperations with other States to combat transnational supply chain issues. **3.** Increase attention to national policy and in dialogue with other States and relevant actors at the United Nations and other forums on how to ensure all States can compete and innovate on an equal footing, so as to enable the full realization of ICTs to increase global social and economic development and contribute to the maintenance of international peace and security, while also safeguarding national security and the public interest.[48]	• International cybersecurity forums and dialogues to exchange information/ideas on norms. • Regular bilateral/multilateral dialogues with States. • Diplomats must be capable of meaningfully engaging with their counterparts on the specific topic of supply chain security.[49]

[47] See OEWG. 2024. Final Substantive Report, Annex A, Norm I (1).

[48] See OEWG. 2024. Final Substantive Report, Annex A, Norm I (7).

[49] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 34.

Norm 13 (j)

Report ICT Vulnerabilities *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*		
PILLARS	**STEPS TO BE TAKEN**	**SUGGESTED CAPACITY-BUILDING ACTIVITIES**
POLICY	**1.** Develop the State's strategy and approach to support responsible reporting of ICT vulnerabilities. **a.** As a start, States could implement a process to timely report discovered vulnerabilities as well as remedies to existing threat repository platforms as part of information sharing. **b.** Develop Framework / SOPs of Confidentiality to ensure responsible and impartial reporting to existing threat repository platforms. **c.** It is recommended to form this policy with a multi-stakeholder approach, such as including tech companies in national ICT vulnerability reporting initiatives. **d.** This policy should also encourage and support individuals such as independent security researchers and penetration testers to participate in responsible disclosure of ICT vulnerabilities. **2.** Put in place vulnerability disclosure policies and programmes including a coordinated vulnerability disclosure process to minimize the harm to society posed by vulnerable products and systematize the reporting of ICT vulnerabilities **3.** Conduct periodic reviews of the strategies to ensure that they are relevant and applicable to the evolving geopolitical and cybersecurity landscapes. **4.** Ensure that new and updated strategies are appropriately disseminated to the relevant parties.	• Cross-border collaboration with other States and international unions to learn about best practices on how to govern and manage ICT vulnerabilities. • Public communication skills especially when it is vital to address the general public about vulnerabilities that impact the population.[50]
OPERATIONAL	**1.** Appoint relevant agencies or divisions to oversee the management of ICT vulnerabilities in the State. **2.** Establish a national CERT/CSIRT. **3.** Assign a contact point to the national CERT/CSIRT to allow the public or organizations to report vulnerabilities to the national CERT/CSIRT to investigate and follow up.	• CERT/CSIRT capacity-building programmes. • Incident response training courses. • Collaborating with other States and international unions to learn about best practices on how to govern and manage ICT vulnerabilities.

[50] Ibid., 36.

OPERATIONAL	**4.** For confirmed vulnerabilities, the national CERT/CSIRT should take appropriate steps to share this information with threat/information repositories in line with the Regional Framework of Confidentiality. **5.** Establish a dedicated office within the government who will oversee the management of ICT vulnerabilities at the national level. **a.** This office should maintain links with the various critical infrastructures (CIs), critical information infrastructures (CIIs), and industry stakeholders to allow for efficient reporting, coordination, mitigation, and patching of vulnerabilities. **b.** This office should develop and maintain a framework / mechanism to facilitate the efficient reporting, coordination, mitigation and patching vulnerabilities with researchers and penetration testers. **6.** Set up a Vulnerability Disclosure Programme (VDP) for the government's ICT systems to provide clear guidelines on responsible vulnerability disclosure. **a.** The VDP should clearly state the boundaries that penetration testers must adhere to, otherwise they will be in breach of the law. **b.** The VDP should also be as transparent as possible. For instance, detailing the entire disclosure process will give vulnerability reporters a better idea of the VDP. **7.** Assist and support CI and CII owners to set up their respective VDPs. **a.** The office identified in Step 5 should also be involved in these VDPs to monitor for malicious cyber operations at the national level. **8.** The office identified in Step 5 should manage a system to escalate confirmed vulnerabilities identified through Steps 6 and 7 to vendors of affected products for the latter to follow-up and resolve disputes, if any. **a.** For instance, the office can notify the national CERT/CSIRT, which forwards the information to the respective vendors. **9.** Create a national 'response/escalation mechanism' in the event that a discovered vulnerability impacts a CI or CII. **a.** It is recommended to have a tiered-response system to have different responses based on the severity of the vulnerability.	

OPERATIONAL	**10.** Set up bug bounty programmes for educational institutions and the public to participate in. Such programmes are mutually beneficial: **a.** Skilled cybersecurity professionals can help to identify vulnerabilities in systems in CIs and CIIs. **b.** Participants can use such programmes as opportunities to build their portfolios and career. **c.** Build local talent for cybersecurity. **d.** Create awareness about cyber vulnerabilities and cybersecurity to the public. **11.** Engage with established cybersecurity companies or big tech companies to tap on their expertise on cybersecurity. **a.** This could include employing their services to conduct vulnerability assessments and penetration testing on CI and CII systems. **12.** Partner with vendors on ways to address and secure the vulnerabilities. **13.** Issue up-to-date advisories and reports online through different channels (e.g., CERTs/CSIRTs, social media). **14.** Publish annual CERT/CSIRT reports to create awareness of the latest cyber landscape and cyberattack trends.	
TECHNICAL	**1.** Identify the infrastructure and technologies needed to help assist in ICT vulnerability reporting and management (e.g. strong network infrastructure, sandboxing systems for analysis). **2.** Design and implement the infrastructure based on cybersecurity principles and requirements specified in international standards and best practices. **3.** Perform security testing comprising Source Code Review, Vulnerability Assessment (VA) and Penetration Testing (PT). **4.** Promote and support local cybersecurity talent to take up technical certifications in offensive security to hone their skills.	• Conferences or trade exhibitions to keep updated on latest technological offerings. • Working with the private sector to implement the required infrastructure, hardware, and software.

LEGAL	**1.** Train government officers with legal/judicial responsibilities to be versed in the legal aspects of cyber. **2.** Consider the feasibility of introducing legislation that supports responsible vulnerability reporting. **a.** Ensure that the integrity of critical infrastructure (CI) and critical information infrastructure (CII) systems are protected while giving researchers/public the ability to carry out vulnerability testing responsibly. **b.** Provide adequate protections to researchers and penetration testers[51] who are disclosing vulnerabilities with no malicious intent. **c.** Provide appropriate legal and financial safeguards to bug bounty programmes.	• Courses on the application of local and international laws in cyberspace, in relation to the reporting of ICT vulnerabilities. • Courses that prepare States to implement cyber-related legal frameworks into their own legislations. • Regional and international forums and dialogues on cyber laws.
DIPLOMACY	**1.** Participate in relevant regional and international forums to learn and exchange information about existing and emerging threats related to the ICT industry. **2.** Establish mutual agreements with other States to exchange information about reported vulnerabilities. **3.** Consider coordinated vulnerability disclosure with partners.	• International cybersecurity forums and dialogues to exchange information/ideas on norms. • Regular bilateral/multilateral dialogues with States.

[51] See OEWG. 2024. Final Substantive Report, Annex A, Norm J (4).

Norm 13 (k)

Protection of CERTs *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*		
PILLARS	**STEPS TO BE TAKEN**	**SUGGESTED CAPACITY-BUILDING ACTIVITIES**
POLICY	**1.** Establish a National CERT/CSIRT Framework **a.** Consider declaring CERTs/CSIRT part of national critical infrastructure. **b.** Define the roles and responsibilities of CERTs/CSIRTs. **c.** Create sectoral CERTs/CSIRTs for each CI/CII. **d.** Categorize CERTs/CSIRTs (e.g. national, sectoral, organizational). **e.** Consider the establishment of ad-hoc CERTs/CSIRTs for specific incidental purposes. **f.** Establish escalation procedures, where appropriate. **g.** CERTs/CSIRTs should not be politically affiliated. **2.** Issue a list of all declared CSIRT/CERTs on their territory.[52] **3.** 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).[53] **4.** Formulate a policy for the categorization of CERTs/CSIRTs as part of national critical infrastructure. [54] **5.** Outline in cybersecurity policy and/or strategy the clear status, authority and mandates of the CERTs/CSIRTs (which distinguish their unique neutral functions from other government functions).[55]	• Collaborating with other States and international unions to learn about best practices on how CERTs/CSIRTs can be protected from harm.

[52] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 37.

[53] Ibid.

[54] See OEWG. 2024. Final Substantive Report, Annex A, Norm K (1).

[55] See Samuele Dominioni and Giacomo Persi Paoli, 2023. Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, p. 37.

POLICY	6. Conduct periodic reviews of the frameworks to ensure that they are relevant and applicable to the evolving geo-political and cybersecurity landscapes. 7. Ensure that new and updated frameworks are appropriately disseminated to the relevant parties.	
OPERATIONAL	1. Establish/appoint a national CERT/CSIRT to handle cyber incidents at the national level. 2. Establish a code of conduct for CERT/CSIRT members on how to carry out their duties. a. The code of conduct could remind members not to engage in offensive cyber acts. 3. Develop playbooks and SOPs for cyber incident management under various ops environments or affected systems at the national level. 4. Gain membership in regional and international CERT/CSIRT networks. 5. Have the national CERT/CSIRT participate in CERT-related trainings to build capacity. 6. Have the national CERT/CSIRT participate in regional and international CERT/CSIRT networks. a. Exchange information and mitigation for incidents. b. Build trust by establishing points of contact for bilateral cooperation.	• CERT/CSIRT capacity-building programmes. • Incident response training courses. • Exchanging best practices with other CERTs/CSIRTs on how to protect one's on infrastructure. • Code of conduct/ethics training courses and awareness programmes.
TECHNICAL	1. Determine and implement possible protection mechanisms that could help protect national CERT/CSIRT systems from cyberattacks. 2. Support CERT/CSIRT members to get certifications that will be useful in cyber incident management duties.	• Conferences or trade exhibitions to keep updated on the latest technological offerings. • Working with the private sector to implement the required infrastructure, hardware, and software.
LEGAL	1. Train government officers with legal/judicial responsibilities to be versed in the legal aspects of cyber. 2. Study the feasibility of introducing legislation that protects CERTs/CSIRTs from malicious actions that may impede their work.	• Courses on the application of local and international laws in cyberspace. • Courses that prepare States to implement cyber-related legal frameworks into their own legislations. • Regional and international forums and dialogues on cyber laws. • Legal expertise, including in international law specific to the ICT domain which is key to properly implementing several elements (e.g., to draft the national interpretation of the norm) pertaining to the implementation of the norm.[56]

[56] Ibid., 38.

DIPLOMACY	**1.** Encourage the State to make public statements and commitments that the State will not use the CERT/CSIRT for any malicious activity. **a.** This could also be an opportunity to request other States to likewise not impede the work of its national CERT/CSIRT by attacking its ICT systems. **2.** Work with regional and international organizations to recognize the importance of a CERT/CSIRT's work as a neutral entity working to protect critical infrastructure (CI) and critical information infrastructure (CII). **a.** This can be a catalyst for the international community to introduce additional measures to further protect the work of CERTs/CSIRTs.	• International cybersecurity forums and dialogues to exchange information/ideas on norms. • Regular bilateral/multilateral dialogues with States.


asean