PUTTING CYBER NORMS IN PRACTICE:

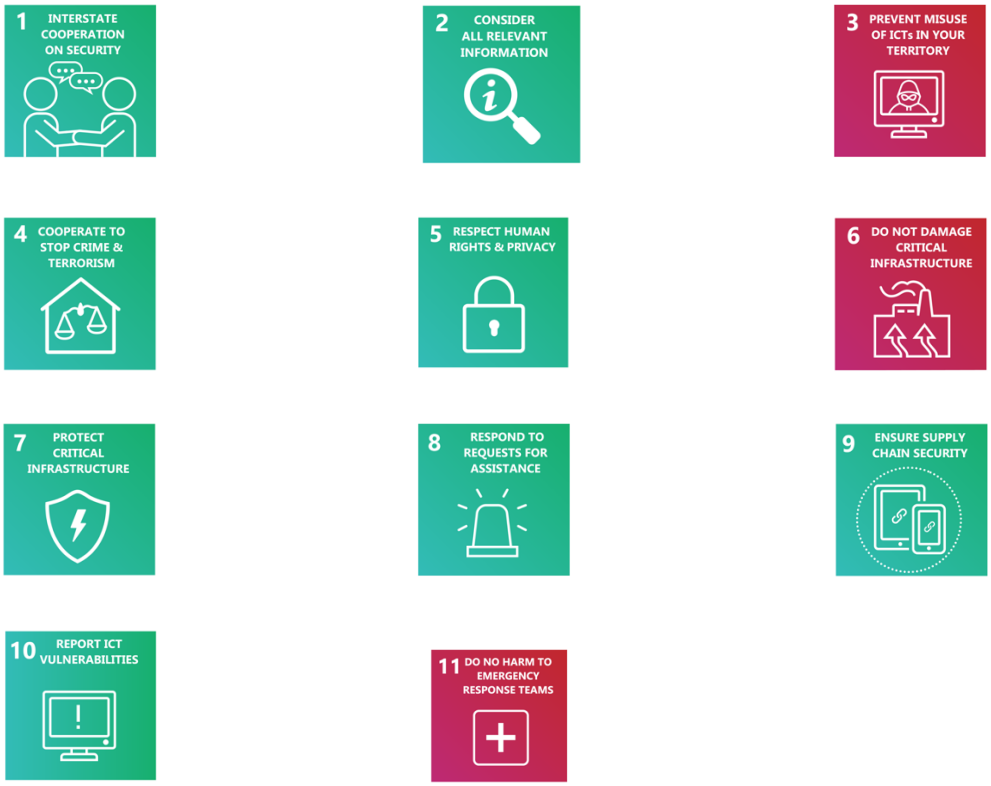
Implementing the UN GGE 2015 recommendations through national strategies and policies

Mika Kerttunen
Eneken Tikk

2021

[this page intentionally left blank]

Table of Contents



UN Norms of Responsible State Behaviour in Cyberspace:
Icons provided by the Australian Strategic Policy Institute

Source: https://www.aspi.org.au/cybernorms/downloads

This is an academic research report that was commissioned by the Global Forum on Cyber Expertise (GFCE) as part of its Global Cyber Capacity Building Research Agenda 2021. The project was sponsored by the United Kingdom (UK) Foreign and Development Office (FCDO) and the research was conducted by Eneken Tikk and Mika Kerttunen.

The information, interpretation and examples set out in this paper do not constitute official or informal opinions or positions of the GFCE, its Secretariat, its members and partners, the project sponsor, or any other government. Neither the GFCE nor its members may be held responsible for the use which may be made of the information contained therein.

Through the Global Cyber Capacity Building Research Agenda mechanism, the GFCE aims to identify and address knowledge gaps relevant to ongoing GFCE work and members' capacity building activities. For this research project, the topic was identified in 2020 by members of the CBMs/Norms Implementation and Cyberdiplomacy Task Force under the Working Group on Cybersecurity Policy and Strategy.

More information about the Working Group can be found on the GFCE website.

Introduction

Every country has a unique path for maximizing both the potential and the benefits of information and communication technologies (ICTs) for national purposes and aspirations. Thus, every country has a unique formula for implementing the recommendations in the 2015 report of the UN's Group of Governmental Experts (GGE) on "Developments in the field of information and telecommunications in the context of international security". Between 2019 and 2021, the GGE elaborated it's 2015 report, which the UN's Open-ended Working Group (OEWG) endorsed in its 2021 Final Substantive Report. All countries are also experiencing different phases of digital development. Some are establishing the elementary framework, infrastructure and baseline capabilities for accommodating ICTs as part of their societal fabric. Others are revising or renewing existing solutions and models to further enhance and maximize the use of ICTs for national goals and purposes. Still others have become highly dependent on ICTs in and are seeking for ways to fully integrate digital products and services in their daily activities. Because each country has its own starting point, goal and trajectory for implementing the UN's GGE 2015 recommendations, our Implementation Guide introduces various approaches that can be, and have been, adopted to implement norms of responsible state behaviour. The Implementation Guide seeks to facilitate, inform and promote collaborative and coordinated efforts to maintain and further develop an open, free, peaceful and stable cyberspace through adequate national, regional and global cybersecurity practices.

Implementation of the GGE's recommendations requires adjusting or establishing policies, procedures, regulations or capabilities or adopting other measures which support state and national adherence to the projected conditions of the recommendations for norms. In the OEWG's 2021 Final Substantive Report, countries have committed to support the implementation and development of norms of responsible state behaviour in partnership with relevant organizations including the UN. By improving national cybersecurity, countries will be better able and willing to work with other countries to improve cybersecurity regional and globally. Coherence of implementation strengthens international peace and security through cooperation and enhanced domestic cybersecurity. Our research emphasizes that countries have, even before the GGE's guidance, started heading in the right direction and every country has already implemented some of the recommended steps. Although, the initial national steps may have been taken without explicit international peace and security considerations, they serve as foundations for implementing the recommendations. Additional impetus may be needed to achieve the objectives of international peace and security.

Successful and comprehensive implementation of any recommendation inevitably requires commitment and progressive steps from several authorities and agencies. Consequently, implementation practice will comprise unique and contingent combinations of legislative, doctrinal, organizational and technical-material resources and measures. Accordingly, only combinations of activities or implementation ideas can be taken to represent the full scope of a recommendation. Indeed, governments are encouraged to conduct comprehensive operationalization analysis of the recommendations. This is particularly essential to be able to tailor domestic measures to serve the purposes of international peace, security, and stability.

Moreover, domestic implementation of these global, multifaceted recommendations will require effective coordination and indeed harmonization of state and governmental action, which will enable countries to follow their respective national political-administrative principles, procedures, and structures. Still, other countries' implementation practices can offer direction and inspiration. Advancing

international peace and security requires anchoring relevant measures and activities on national security and cybersecurity governance frameworks.

This Implementation Guide is structured as follows. For each GGE 2015 recommendation, our substantive guidance chapter begins with the GGE's 2019-2021 implementation guidance. This is followed by three key elements which exemplify how the theme and direction of respective recommendations have been adopted in national strategies and policies guiding digital development, national information security and cybersecurity. Pertinent cameos tell national stories with special focus on the recommendation in question. Further national examples illustrate how the recommendations can be implemented in various national contexts and formats involving (i) political and normative statements; (ii) adopting national legislation; (iii) establishing operational entities; (iv) developing material and immaterial capacities and (v) cooperating with and assisting friends, partners and neighbours. At the end of each section, we offer consolidated good practices for implementing the particular recommendation. This guidance is based on practices within the scope of each recommendation, opinions on and the submission (to the UN Secretary General, and the GGE's and OEWG's processes) specific to each country, as well as on expert commentary representing various aspects of national and international cybersecurity.

This collection of national examples is not exhaustive. It is intended to offer insights and inspiration. The substantive guidance chapter is essentially an open catalogue where examples of national efforts and successes can be added over time. By exchanging views and experience on implementing the recommendations, countries establish durable practices, structures and relationships, patterns of normalcy rather than exception. We would like to encourage countries to share their implementation methods.

The procedural guidance chapter offers considerations for getting started or advancing established processes. A first step towards implementation is acknowledgment that the GGE's recommendations on responsible state behaviour are ways to improve national cybersecurity. Most countries have already endorsed the recommendations through regional and international processes, confirming their overall value for improving national and international cybersecurity. The second step, we suggest, should bring the GGE's recommendations to the awareness of further national stakeholders – other government entities, NGOs and the private sector and the population. This step is a valuable discussion starter about where a nation can start to develop its cybersecurity strategy and which goals to set.

At the end of the Implementation Guide, there is a bibliography of relevant UN documents and other works advising how to implement the GGE's 2015 recommendations.

Recommendation 1: Interstate 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.

GGE 2021 Guidance:

- The maintenance of international peace and security and international cooperation are among the founding purposes of the United Nations. This norm is a reminder that it is the common aspiration and in the interest of all States to cooperate and work together to promote the use of ICTs for peaceful purposes and prevent conflict arising from their misuse.

- In this regard, and in furtherance of this norm, the Group encourages States to refrain from using ICTs and ICT networks to carry out activities that can threaten the maintenance of international peace and security.

- The measures recommended by previous GGEs and the OEWG represent an initial framework for responsible State behaviour in the use of ICTs. As further guidance, and to facilitate such cooperation, the Group recommends that States put in place or strengthen existing mechanisms, structures and procedures at the national level such as
    - relevant policy, legislation and corresponding review processes;
    - mechanisms for crisis and incident management;
    - whole-of-government cooperative and partnership arrangements;
    - and cooperative and dialogue arrangements with the private sector, academia, civil society and the technical community.

  States are also encouraged to compile and streamline the information they present on the implementation of the norms, including by voluntarily surveying their national efforts and sharing their experiences.

Elements of implementation

To successfully implement this recommendation, states could consider focusing on cooperation, stability enhancing measures and best security practices. The following examples demonstrate how states and organizations have prioritized these elements.

COOPERATION

Malaysia will innovate proposals on international cyber security cooperation tailored to the interest of the respective fora in collaboration with the identified partners. Concurrently, Malaysia will also promote international collaboration in both the public and private sectors and engage with trusted and international partners and entities that share the same vision.

Malaysian Cyber Security Strategy 2020-2024 (2020)

STABILITY ENHANCING MEASURES

Jordan seeks to build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability. National action to be taken include brokering international and regional agreements on cyber intelligence sharing and influencing international cyber security policies.

Jordan National Cyber Security Programme (2018)

BEST SECURITY PRACTICES

The Economic Community of West African States member states have adopted a regional strategy to improve the level of national cybersecurity and cybercrime mechanisms, and to develop cooperation and mutual assistance between the countries of the region. Drawing on internationally recognized best practices, the Regional Strategy includes detailed objectives to strengthen cybersecurity for a safe and secure cyberspace.

ECOWAS Regional Cybersecurity and Cybercrime Strategy (January 2021)

Close-up: PORTUGAL

A systemic approach to cooperation to increase stability and security

The Portuguese *National Strategy for Cyberspace Security 2019-2023* establishes a clear linkage between international cooperation and national endeavours to strengthen domestic cybersecurity.

"[The] Strategy calls for an enhanced duty of cooperation between national structures and entities with responsibility in areas contributing to the security of cyberspace, whether public or private. At the same time, it promotes Portugal's international action, both bilaterally and multilaterally, in order to deepen the solid network of existing alliances, to exert influence by affirming its presence in the world and empowering others through strategic partnerships, namely between Portuguese speaking countries, thereby actively contributing to shaping the international ecosystem while safeguarding the national interest. Additionally, it is important to characterize the national participation in the various cyber defence activities in the international context in which Portugal operates, which allow the aggregation of knowledge and experience, also enabling the national affirmation in this field."[1]

The *National Strategy for Cyberspace Security Strategy* sets a number of tangible measures for implementation:

Axis 1. Cyberspace security structure:

- Strengthen the National Cybersecurity Centre as the National Cybersecurity Authority and, as a result, as the national single point of contact for international cybersecurity cooperation purposes
- Update the Public Prosecution structures through the establishment of specialized response structures for emerging requests arising from crimes in the digital environment to ensure evidence-based effectiveness and to be able to meet potential international cooperation requirements in criminal matters
- Strengthen the capacities of the Criminal Police by strengthening its structures and human and technical capacities for investigating and combating cyber-crime by fostering the human resources allocated to this area and its ability to carry out evidence-taking measures using technical means, and to respond to the requirements of the international cooperation of the police
- Strengthen the Security Intelligence Service as well as the Strategic Defence Intelligence Service so that their human and technical research and analysis resources can have a clear picture of the capabilities and intentions of threat vectors that are being identified at all times, while strengthening international cooperation and consolidating proximity with national actors in this field
- Develop, within the scope of the international action, cyberdiplomacy as the discipline of the State's external action aimed at promoting, inter alia, the application of the existing international law to cyberspace in order to ensure its stability, the transparent and shared governance of its universal use and the efficient creation of normative capacities, namely within the Portuguese-Speaking Countries Community.[2]

[1] Resolution of the Council of Ministers No. 92/2019. *Portuguese Official Journal*, Series 1:108 (5 June 2019).
[2] Resolution of the Council of Ministers No. 92/2019. *Portuguese Official Journal*, Series 1:108 (5 June 2019), Axis 1: Cyberspace security structure.

Axis 6. National and international cooperation:

- Contribute to the regulation and universalization of the cyberspace by promoting the respect for the applicable international law, the transparent sharing of its governance among all actors, their universal accessibility and the dissemination of good usage practices
- Deepen the national participation in the relevant bodies, organisations and agencies, also in the effort to reduce the risk of inter-state tensions within cyberspace security
- Participate in cybersecurity and cyber defence exercises by strengthening and increasing the level of maturity for cyberspace protection, where sharing information and knowledge is a key factor
- Integrate international cyber security and cyber defence organizations with a view to international cooperation and the affirmation of Portugal in this field
- Develop the international cyber-discipline framework in which Portugal should be inserted, identifying priority initiatives, namely the international or intergovernmental organizations for the exchange of good practices to which it should adhere.[3]

Examples how Portugal is implementing its international and cooperative ambitions, include measures to be taken during the Portuguese EU Council presidency (January – June 2021):

- Monitoring the initiatives arising from the new Security Union Strategy and giving priority to the development of the new internal security strategy for the EU Based on prevention and the protection of citizens and their rights, freedoms and guarantees
- Strengthening the capacity of law enforcement and judicial bodies to identify and mitigate new criminal and cybersecurity threats,
- In the framework of EU-NATO cooperation, paying particular attention to the areas of hybrid threats, cyber defence, maritime security (including capacity-building for partners), military mobility and response to complex emergencies
- From a cooperative security perspective, seeking to deepen synergies with relevant regional entities in North Africa, the Middle East and the Sahel
- Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres,
- Completing of a 2017 proposal on 'e-Privacy on the respect for private life and the protection of personal data in electronic communications' (2017/0003(COD)).[4]

[3] Resolution of the Council of Ministers No. 92/2019. *Portuguese Official Journal*, Series 1:108 (5 June 2019), Axis 6: National and international cooperation.

[4] *Programme for the Portuguese Presidency of the Council of the European Union*. https://www.2021portugal.eu/media/e0rjnvdj/programme-for-the-portuguese-presidency-of-the-council-of-the-european-union-en.pdf; and Directorate-General for the Presidency (2021) "Priority dossiers under the Portuguese EU Council Presidency." Lucienne Attard (ed.). European Parliamentary Research Service.

Further examples of implementation

SOUTH AFRICA National Cybersecurity Policy Framework (2015)	The South African *National Cybersecurity Policy Framework* (2015) represent widely shared sentiments on cybersecurity and the importance of taking global and national action: The numerous cyber-attacks launched in recent years against advanced information societies aimed at undermining the functioning of public and private sector information systems have placed the abuse of cyberspace high on the list of international and also local security threats. Given the seriousness of cyber threats and of the interests at stake, it is therefore imperative that the comprehensive use of information communication technology solutions be supported by a high level of security measures and be embedded in a broad and sophisticated Cybersecurity culture. For this reason, the cyber threats need to be addressed at both the global and national levels.[5]
JAPAN Cybersecurity Strategy (2018)	The Japanese government promotes public and private sector initiatives on cybersecurity based on three approaches (1. mission assurance of service providers; 2. risk management; and 3. participation, coordination and collaboration) with the aim of autonomous and sustainable evolution and development of reliable cyberspace while realizing both security and economic development in cyberspace.[6]
DOMINICAN REPUBLIC Estrategia Nacional de Ciberseguridad 2018-2021 (2018)	The National Cybersecurity Strategy 2018-2021 of the Dominican Republic dedicates its fourth pillar to fostering alliances between the public and private sectors, as well as with civil society and international organizations and institutions to cooperate in cybersecurity matters. This is done by adopting relations with international organizations and institutions to facilitate cross-border cooperation and creating more confidence in the area of incident response and in international collaboration and information exchange. To achieve this the country has proposed: - Promoting bilateral and multilateral agreements for cooperation, exchange of experiences and information related to cybersecurity - Ensuring the participation of the Dominican Republic in international forums on cybersecurity - Identifying countries with research and development objectives similar to those as the Dominican Republic and promoting the exchange of information and knowledge with them.[7]

[5] State Security Agency (2015). *National Cybersecurity Policy Framework for South Africa*, p. 5.
[6] Cabinet Office (Japan) (2018). *Cybersecurity Strategy,* p. 11-12.
[7] Dominican Republic (2018). Artículo 8, Pilar 4, "Alianzas Nacionales e Internacionales."

CHILE National Cybersecurity Policy (2017)	How individual states are addressing international cooperation can be found, for instance, in the Chilean (2017) *National Cybersecurity Policy*: One of the high-level objectives of this policy relates with the international relations and cooperation about cybersecurity in the global context. However, it is essential for the country to incorporate these and other objectives, such as the development of human rights, defence, and other related objectives in order to consolidate and integrate the same into Chile's foreign policy.[8]
BRAZIL Estratégia Nacional de Segurança Cibernética (2020)	Brazil's commitment from 2020 reads as: It should be noted that cybersecurity is a global issue in which interaction between various actors in the international community is paramount for the construction of a secure and reliable digital environment. In this sense, it is recommended that Brazil adopts guidelines that, through confidence-building measures, aim at interstate cooperation, intense exchange of information, transparency, predictability of actions, reaffirmation of international peace and stability, in a way that supports the reduction of the risk of escalation of cyber incidents globally.[9]
MALAYSIA Cyber Security Strategy 2020-2024 (2020)	*Malaysian Cyber Security Strategy 2020-2024* (2020) contains a wide array of targeted commitments, including: Malaysia will also strive to be at the forefront of international discussions by driving, chairing and hosting regional and international cyber security fora as well as conferences.[10]
AUSTRALIA Cyber Security Strategy (2020)	*Australia's Cyber Security Strategy* (2020), among other instruments, is determined to impose consequences to secure stability and prevent malicious practises: The Australian Government will deter malicious activity by imposing stronger consequences for those who act contrary to existing international law and agreed norms when it is in Australia's national interest to do so.[11]
SWITZERLAND Reply to the UN Secretary-General (2016)	The Swiss National Cybersecurity Strategies of 2012 and 2018-2022 acknowledge the importance of ICTs as indispensable drivers of social, economic, and political activities, and they lay the foundation for a comprehensive, integrated and holistic approach to address ICT-based threats. Switzerland seeks to improve its early detection of cyber risks and emerging threats, increase resilience of its critical infrastructure and generally reduce cyber risks. The strategies' underlying rationale is the need

[8] Gobierno de Chile (2017). *National Cybersecurity Policy,* p. 13 and 15.
[9] Presidência da República (2020). *Estratégia Nacional de Segurança Cibernética*, p. 38.
[10] National Security Council (2020). *Malaysian Cyber Security Strategy 2020-2024,* p. 80-81.
[11] Australian Government (2020). *Australia's Cyber Security Strategy 2020*, p. 41.

	for a cyber security culture, shared responsibility between different levels of government and between the public and the private hand as well as the need for a risk-based approach. They advocate a stronger coordination at the governmental level, foster private-public partnerships and enhanced cooperation in the international arena. Cooperation, whether at the national or international level, was defined as one of the cornerstones of the Swiss approach to tackle cyber threats. Furthermore, Switzerland is convinced that application of international law including human rights law and international humanitarian law, voluntary non-binding norms, confidence building measures and capacity building are key to ensuring and maintaining international cybersecurity.[12]
ASEAN Norms Implementation (2020)	The Association of Southeast Asian Nations (ASEAN) has developed ASEAN 2020 ICT Masterplan as well as ASEAN Cybersecurity Strategy. Southeast Asia has taken steps beyond mere endorsement of the UN GGE 2015 report. ASEAN states have together started systematic work for implementing the experts' recommendations.[13]
OSCE Confidence-Building Measures (2013, 2016)	The participants of the Organization for Security and Cooperation in Europe (OSCE; 2013 and 2016 decisions) have developed region-specific confidence-building measures "to enhance interstate cooperation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.[14]" These measures build on the spirit and letter of the UN GGE 2010, 2013 and 2015 reports.
The Pacific Island Forum The Boe Declaration (2018)	The Pacific Island Forum (PIF) 2018 "Boe Declaration" reaffirmed the importance of the rules-based international order and adherence to relevant international law and resolution of international disputes by peaceful means. The PIF nations have expanded the concept of security to include cybersecurity for the purpose of maximizing "protections and opportunities for Pacific infrastructure and peoples in the digital age."[15]

[12] Federal Department of Foreign Affairs (2021). Resolution 75/32 on "Advancing responsible State behaviour in cyberspace in the context of international security." Submission to the report of the United Nations Secretary-General (27 May).
[13] Cyber Security Agency of Singapore (2020). "Opening Speech by Mr S. Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity." ASEAN Ministerial Conference on Cybersecurity 2020. *https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2020*.
[14] Organization for Security and Co-operation in Europe (2016). Permanent Council Decision No. 1202 OSCE Confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. (10 March 2016).
[15] Pacific Island Forum (2018). "Boe Declaration on Regional Security." https://www.forumsec.org/2018/09/05/boe-declaration-on-regional-security/

Considerations for practice

- Determine ICT issues that are critical for national development and lines of cooperation that are needed to resolve relevant issues. Make sure that national strategies, policies and action plans consider the appropriate roles and responsibilities of various stakeholders and establish clear lines of interaction and collaboration. Where cross-border, interagency or cross-sector collaboration and activities are necessary, integrate national cybersecurity policies and strategies with other national, e.g. foreign policy, trade, defence.

- Determine threats and risks for national cybersecurity. Make sure that national cyber/ICT incident prevention frameworks, including computer emergency response capability and ICT crisis coordination mechanisms are included in collaborative frameworks and have clear procedures and guidance for cooperation.

- Determine the factors that make harmful uses of ICTs more likely or likely to be successful. Share your observations with national stakeholders. Compare your findings with other countries to support international dialogue and measures to prevent harmful ICT practices.

- Consider best practices in national cybersecurity and share your experience with other countries to discuss and determine measures that increase stability and security in the use of ICTs. Relevant regional dialogues, coordination and cooperation can further inform global cooperation on best cooperative cybersecurity processes, practices and mechanisms.

- Determine the need for additional information and expertise and promote national capacity and competences that can support regional and international efforts. Contribute to international and regional dialogues and processes directed at developing normative and other measures of cybersecurity and stability.

- Develop and/or build on existing interstate relations within bilateral or plurilateral fora to engage on national and international ICT developments. Cyber dialogues as part of exiting bilateral relations are good starting points to establish areas of mutual concern and priority.

Recommendation 2: 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.

GGE 2021 Guidance:

- This norm acknowledges that attribution is a complex undertaking and that a broad range of factors should be considered before establishing the source of an ICT incident. In this regard, the caution called for in paragraph 71 (g) of this report and in previous GGE reports can help avert misunderstandings and escalation of tensions between States.

- States that are subject to malicious ICT activity, and States from whose territory such malicious ICT activity is suspected to have originated, are encouraged to consult among relevant competent authorities.

- A State that is victim of a malicious ICT incident should consider all aspects in its assessment of the incident. Such aspects, supported by substantiated facts, can include the incident's technical attributes; its scope, scale and impact; the wider context, including the incident's bearing on international peace and security; and the results of consultations between the States concerned.

- An affected State's response to malicious ICT activity attributable to another State should be in accordance with its 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. States could also avail of the full range of diplomatic, legal and other consultative options available to them, as well as voluntary mechanisms and other political commitments that allow for the settlement of disagreements and disputes through consultation and other peaceful means.

- To operationalize this norm at the national level and facilitate the investigation and resolution of ICT incidents involving other States, States can establish or strengthen relevant national structures, ICT-related policies, processes, legislative frameworks, coordination mechanisms, as well as partnerships and other forms of engagement with relevant stakeholders to assess the severity and replicability of an ICT incident.

- Cooperation at the regional and international levels, including between national Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs), the ICT authorities of States and the diplomatic community, can strengthen the ability of States to detect and investigate malicious ICT incidents and to substantiate their concerns and findings before reaching a conclusion on an incident.

- States can also use multilateral, regional, bilateral and multi-stakeholder platforms to exchange practices and share information on national approaches to attribution, including how they distinguish between different types of attribution, and on ICT threats and incidents. The Group also recommends that future work at the United Nations could also consider how to foster common understandings and exchanges of practice on attribution.

Elements of implementation

To successfully implement this recommendation, states could consider focusing on incident reporting templates, incident management and larger context of the event. The following examples demonstrate how states and organizations have prioritized these elements.

INCIDENT REPORTING TEMPLATES

Cambodia Computer Emergency Response Team (CamCERT) has adopted an initial incident reporting template. The information requested about an incident includes:

- The time of occurrence of the incident (timestamp)
- Information regarding effected system or network
- Part of log files information
- Relevant technical information such as security system deployed, actions taken to mitigate the damage and
- Suspected method.

Cambodia Computer Emergency Team (2021) "Report Incident."

INCIDENT MANAGEMENT

The Government of Bangladesh Information Security Manual (GOBISM, 2017) contains detailed guidance to government agencies on cyber incident management. GOBISM functions as a set of information security principles and measures that could be transposed into Government legal acts, policies and standards and a framework of controls for accreditation and certification of government systems.

Government of Bangladesh Information Security Manual (GPBISM) (2017)

LARGER CONTEXT

When considering attribution, the UK Government will consider, alongside a technical assessment from the National Cyber Security Centre, the geopolitical and bilateral factors: our wider objectives towards the State in question, including national security objectives, regional stability, the sensitivities of our allies and the likelihood of counter-response.

FCO (2019) Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015.

Close-up: UNITED KINGDOM

A comprehensive framework for incident handling

The United Kingdom 2016 *National Cyber Security Strategy* linked the public attribution of cyber attacks to national interest: "To reduce the cyber threat from hostile foreign actors, we will: attribute specific cyber identities publicly when we judge it in the national interest to do so."[16] On the other hand, despite the fact that the techniques used in most cases had not particularly advanced (including exploiting unpatched vulnerabilities and spear-phishing), the 2017 *National Crime Agency* stated that the blurring boundaries between nation states and cyber criminals had made attribution "all the more difficult."[17]

During and after a cyber incident, the intelligence gathered goes into mapping the broader threat landscape. Here, having those who track and those who respond to threat in the same team helps to better understand who is targeting, investigate them and share findings. This can lead to both significant breakthroughs in broader UK intelligence operations and public attribution.[18]

The National Cyber Security Centre (NCSC) assessments were behind attributing WannaCry to the North Korean Lazarus Group and NotPetya to the Russian state.

NCSC Director of Operations Paul Chichester[19]

When considering attribution, the UK Government will consider, alongside a technical assessment from the National Cyber Security Centre:

a. Geopolitical and bilateral factors: our wider objectives towards the State in question, including national security objectives, regional stability, the sensitivities of our allies and the likelihood of counter-response.
b. Impact on victim: the impact of UK attribution (especially public) on the victim(s) of a cyber-incident will be reviewed.
c. Impact on law enforcement activity: the impact of UK attribution (especially public) on the law enforcement investigation of a cyber-incident; for instance the effect on our ability to arrest and prosecute.
d. UK values and ability to operate: attribution should not limit the UK's ability to carry out our own cyber operations in full adherence to domestic and international law. Attribution should be in line with our stated positions in national and international fora, where we champion a free, open, peace and secure cyberspace, and adhere to norms of state behaviour. It should enhance the UK's reputation as a competent cyber actor and weigh up the risk of misattribution.

[16] HM Government (2016). *National Cyber Security Strategy 2016-2021*, p. 49-50.
[17] National Crime Agency (2017). *The cyber threat to UK business*, p. 5, 10.
[18] National Cyber Security Centre (2018). *Annual Review*, p. 22-25.
[19] National Cyber Security Centre (2018). *Annual Review*, p. 25. In December 2017, the Foreign Office Minister for Cyber Security, Lord Ahmad stated, "The UK's NCSC assesses it is highly likely that North Korean Actors known as the Lazarus Group were behind the WannaCry ransomware campaign." In February 2018, the UK, US, and Australian governments publicly attributed the NotPetya cyber attack to the Russian military. Other partners, including Canada and New Zealand, made supportive statements condemning malicious behaviour in cyberspace.

e. Wider response options: the effect of UK attribution on other deterrence activity, which the UK government has agreed or is implementing. The timing of attribution should be calibrated to enhance the impact of other responses.

There are challenges to attribution in cyberspace, but this does not mean it is impossible. Nor should it be viewed in isolation; it is one tool amongst many in a range of options (political, diplomatic, and economic) to respond to malicious cyber activity, with the aim of deterring this activity.[20]

Moreover, when the NCSC assessed that "the GRU was almost certainly (95% +) responsible for defacing websites, cyber-attacks and interruption to TV channels in Georgia in October 2019", the Foreign and Commonwealth Office referred to the *Professional Development Framework for all-source intelligence assessment* used by the UK government for all source intelligence assessments, including the probability yardstick.[21]

[20] Foreign and Commonwealth Office (2019). Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015.

[21] Foreign and Commonwealth Office (2020). "UK condemns Russia's GRU over Georgia cyber-attacks". https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks. The PDF Framework defines the skills required to conduct all-source intelligence assessment as well as makes it easier to understand the function of other parts of the intelligence assessment community. The Framework also outlines Common Analytic Standards to "ensure a consistent standard of rigour, integrity, language and best practice across the UK intelligence assessment community" (Professional Head of Intelligence Analysis (2019) *Professional Development Framework for all-source intelligence assessment.* Crown Copyright, p. 26).

Further examples of implementation

CAMBODIA
Cambodia Computer Emergency Team "Report Incident"
(2021)

For example, Cambodia Computer Emergency Response Team (CamCERT) has adopted an initial incident reporting template. The information requested about an incident includes:

- The time of occurrence of the incident (timestamp)
- Information regarding effected system or network
- Part of log files information
- Relevant technical information such as security system deployed, actions taken to mitigate the damage and
- Suspected method.

Based on the provided information, CamCERT is able to correlate and analyse the incidents, draw inferences and disseminate up-to-date information to relevant parties. This information will also help CamCERT to develop effective security guidelines and prevent occurrence of similar incidents in future.[22]

COLOMBIA
"Reportar un Incidente"
(2021)

Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) has adopted a wider template that includes a taxonomy, categorization [and lexicon] of cyber incidents.[23]

AUSTRALIA
Cyber Incident Management Arrangements for Australian Governments
(2019)

The Australian *Cyber Incident Management Arrangements for Australian Governments* (CIMA) provides Australian Commonwealth, State and Territory governments with guidance on how they will collaborate in response to, and reduce the harm associated with, national cyber incidents. It outlines the inter-jurisdictional coordination arrangements, roles and responsibilities, and principles for Australian governments' cooperation in response to national cyber incidents.

Upon declaring a national cyber incident, the National Cyber Security Committee (NCSC) as the peak cyber security coordination body will activate to support national collaboration and coordination of response efforts. It will provide strategic oversight and coordination of governments' cyber security policies and operational capabilities nationally and national response efforts. The NCSC members (or their representatives) are responsible for leading their jurisdiction's response to a national cyber incident.

The NCSC's role in responding to a national cyber incident includes:

- facilitating the exchange of threat intelligence and solutions to enhance jurisdictions' situational awareness and response activities

[22] Cambodia Computer Emergency Team (2021). "Report Incident." https://www.camcert.gov.kh/en/report-incident/
[23] Grupo de Respuesta a Emergencias Cibernéticas de Colombia (2021). "Reportar un Incidente." http://www.colcert.gov.co/?q=contenido/reportar-un-incidente

- overseeing the development of nationally consistent public information
- providing a forum for consultation that informs members' briefings to their respective senior stakeholders (including Ministers)
- facilitating, where practicable, the sharing of expertise and resources to support jurisdictions' responses.

During a national cyber incident, the Australian Cyber Security Centre will provide technical resources and expertise to jurisdictions that require additional capacity or capability to respond to a national cyber incident and collate, analyse and share information about cyber threats, impacts and mitigation strategies with Australian governments, business and the community.[24]

BANGLADESH
Government of Bangladesh Information Security Manual (GPBISM) (2017)

The Government of Bangladesh Information Security Manual (GOBISM, 2017) contains detailed guidance to government agencies on cyber incident management. GOBISM functions as a set of information security principles and measures that could be transposed into Government legal acts, policies and standards and a framework of controls for accreditation and certification of government systems.[25]

SINGAPORE
Public report of the Committee of Inquiry (2019)

Singapore's cyber incident response framework provides mechanisms for owners of critical information infrastructure (CII) to report, resolve, and recover from incidents affecting CII. Under this framework, and as mandated by the Cybersecurity Act[26], CII owners must report the occurrence of any incident that could potentially affect CII systems to the Cybersecurity Agency of Singapore (CSA).[27] The following details must accompany any incident reporting:[28]

- the CII affected
- the nature of the cybersecurity incident, whether it was in respect of the CII or an interconnected computer or computer system, and when and how it occurred
- the resulting effect that has been observed, including how the CII or any interconnected computer or computer system has been affected
- the incident handling status, including any follow-up actions that have been taken and the next course of action; and
- relevant technical information, including domain names or IP addresses surfaced from the incident.

[24] Australian Signals Directorate (2019). *Cyber Incident Management Arrangements for Australian Governments,* p. 1-4. https://www.cyber.gov.au/sites/default/files/2019-03/cima_2018_A4.pdf.
[25] Government of Bangladesh (2017). *Government of Bangladesh Information Security Manual (GPBISM)*. https://www.cirt.gov.bd/wp-content/uploads/2017/06/GOBISM2.pdf
[26] Republic of Singapore (2018). *Cybersecurity Act. No. 9 of 2018*. https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312#pr14-.
[27] Republic of Singapore (2018). *Cybersecurity (Critical Information Infrastructure) Regulations*. No. s 519. https://sso.agc.gov.sg/SL-Supp/S519-2018/Published/20180830?DocDate=20180830#pr5-.
[28] Cyber Security Agency of Singapore (2020). "Forms." https://www.csa.gov.sg/legislation/forms.

Alongside technical assessments, Singapore takes its national security interest into account when considering whether to publicly attribute incidents such as the SingHealth cyber-attack.[29]

EUROPEAN UNION
GDPR
(2018)

An example of a regional effort is the personal data breach notice requirement in the European Union General Data Protection Regulation. The purpose of requiring data breach notification to both national authorities and individuals whose data has been compromised, is to activate collaborative effort to minimize the adverse effect of the breach.

Companies and other entities who suffer a data breach, are required to (a) describe the nature of the breach; (b) communicate to the national authorities the contact details of their data protection officer; (c) describe the likely consequences of the breach; and (d) identify measures taken or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects.[30] It is expected that such information will be provided without undue delay.

[29] "Statement by Mr S iswaran, Minister-in-Charge of Cybersecurity, on the Government's response to the report of the Committee of Inquiry into the cyber attack on SingHealth, during Parliamentary Sitting on 15 January 2019." https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2019/1/statement-by-mr-s-iswaran-on-govt-response-to-report-of-coi--during-parl-sitting-on-15-jan-2019?pagesize=24&page=12.

[30] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)". *Official Journal of the European Union*, L 119, Volume 59 (4 May 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN,%20Art.%2033%20and%2034.

Considerations for practice

- Establish a framework and mechanisms for ICT incident prevention and management. Facilitate the establishment of industrial and sectorial ICT incident prevention and management capacity. Where possible, support other countries in establishing and developing national ICT incident management capacity and support relevant cooperation.

- Develop national ICT incident detection, mitigation and recovery plan. Conduct regular exercises to test and educate incident detection, mitigation and recovery organizations and personnel. Where possible, participate or arrange bilateral, regional or global ICT incident prevention, mitigation and recovery trainings and exercises.

- Develop situational awareness of political, economic and other factors that may lead to ICT incidents affecting national cybersecurity. Enhance situational awareness through exchanges with industry and other stakeholders. Create mechanisms for coordinated prevention and mitigation. Engage in through bilateral, regional and global exchanges.

- Develop national forensics and other ICT incident investigation capability. Create bilateral, regional and global cooperation mechanisms for prevention, investigation and attribution. Contribute to prevention and attribution efforts bilaterally, regionally and globally.

- Adopt national incident classification and assessment lexicon. Promote bilateral and regional shared understanding of ICT incidents. Contribute to international processes aimed at common understanding of ICT incidents.

- To improve external services competence to relay and analyse information, develop national diplomatic incident response toolkits in line with nationally and internationally accepted diplomatic tools for prevention, deterrence and management.

Recommendation 3: Prevent misuse of ICTs in your territory

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

GGE 2021 Guidance:

- This norm reflects an expectation that if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory it will take all appropriate and reasonably available and feasible steps to detect, investigate and address the situation. It conveys an understanding that a State should not permit another State or non-State actor to use ICTs within its territory to commit internationally wrongful acts.

- When considering how to meet the objectives of this norm, States should bear in mind the following:

    (a) The norm raises the expectation that a State will take reasonable steps within its capacity to end the ongoing activity in its territory through means that are proportionate, appropriate and effective and in a manner consistent with international and domestic law. Nonetheless, it is not expected that States could or should monitor all ICT activities within their territory.

    (b) A State that is aware of but lacks the capacity to address internationally wrongful acts conducted using ICTs in its territory may consider seeking assistance from other States or the private sector in a manner consistent with international and domestic law. The establishment of corresponding structures and mechanisms to formulate and respond to requests for assistance may support implementation of this norm. States should act in good faith and in accordance with international law when providing assistance and not use the opportunity to conduct malicious activities against the State that is seeking the assistance or against a third State.

    (c) An affected State should notify the State from which the activity is emanating. The notified State should acknowledge receipt of the notification to facilitate cooperation and clarification and make every reasonable effort to assist in establishing whether an internationally wrongful act has been committed. Acknowledging the receipt of this notice does not indicate concurrence with the information contained therein.

    (d) An ICT incident emanating from the territory or the infrastructure of a third State does not, of itself, imply responsibility of that State for the incident. Additionally,

notifying a State that its territory is being used for a wrongful act does not, of itself, imply that it is responsible for the act itself.

Elements of implementation

To successfully implement this recommendation, states could consider focusing on situational awareness, feasible measures and notification. The following examples demonstrate how states and organizations have prioritized these elements.

SITUATIONAL AWARENESS

It is recognized that awareness at the national level constitutes a pre-requisite for effective protection in cyberspace. The Government of the Republic of Trinidad and Tobago will assume a leadership role in developing a culture of cyber security. This will necessitate the adoption of a multi-disciplinary and multi-stakeholder approach inclusive of awareness-raising, embedding cyber security in the wider aspects of policy formulation and educating all users of ICT and the Internet on their respective roles in cyberspace.

Trinidad and Tobago National Cyber Security Strategy (2012)

FEASIBLE MEASURES

The State of origin must take appropriate action to terminate [harmful cyber activity], as well as to investigate the incident and bring those responsible to justice. In order to be able to do this, States should have the necessary procedural and legal mechanisms in place. It should nevertheless be recalled that due diligence is an obligation of conduct, not one of result. In general, what is required of States is that they take all measures that are feasible under the circumstances.

International law and cyberspace Finland's national positions (2020)

NOTIFICATION

A State may gain knowledge of such an act following a notification from an affected State. Such notification must be made in good faith and should be accompanied with supporting information. Supporting information may include sharing possible Indicators of Compromise (IoCs), such as IP address and computers used for malicious ICT acts and malware information.
The notified State should acknowledge receipt of the request via the relevant national point of contact.

Canadian submission to OEWG Non-paper, 1 March 2021

Close-up: FINLAND

Determination to prevent internationally wrongful acts

Finland explicitly adheres to the international obligation of due diligence: "States may thus not knowingly allow their territory, or cyber infrastructure within a territory under their control, to be used to cyber operations that produce serious adverse consequences for other States. While only States can violate sovereignty, the sovereignty-based obligation of due diligence extends to private activities taking place in a State's territory."[31]

As how to implement this obligation, Finland's position paper on international law and cyberspace explains that "the State of origin must take appropriate action to terminate [harmful cyber activity], as well as to investigate the incident and bring those responsible to justice. In order to be able to do this, States should have the necessary procedural and legal mechanisms in place. It should nevertheless be recalled that due diligence is an obligation of conduct, not one of result. In general, what is required of States is that they take all measures that are feasible under the circumstances."[32]

Finland is taking thorough measures to avoid her territory and infrastructure being used to commit wrongful acts against other countries. National position and cooperative and domestic measures have been developed through successive information and cybersecurity strategies.

Finland was one of the first countries to issue a national information security strategy. The September 2003 *National Information Security Strategy* aimed at increasing citizens' and companies' trust in the information society and gathered up guidelines and measures that can improve information security and protection of privacy. Despite of the Strategy not referring to international law, it should be noted that the first listed strategic objective of the government was to "promote national and international information security cooperation." Of the key measures in this field, the Strategy lifted up active participation in "the preparation of legislation and standards and other information security cooperation" in the EU, other international organisations and forums in trade and industry.[33]

In a similar mode, the 2013 *Finland's Cyber Security Strategy* noted in several of its 'strategic guidelines' the importance of international participation and cooperation. A particular objective (no. 6/10) focussed on strengthening "national cyber security through active and efficient participation in the activities of international organisations and collaborative fora that are critical to cyber security." For this purpose, international organisations, "such as the UN, the OSCE, NATO and the OECD" were considered important venues for Finland. The EU was recognized being increasingly active in the field of cyber security and also engaging in cooperation with third countries, in which Finland was to participate. In an accompanying dossier, it was noted that "international law handles cyber incidents in a fragmented manner and approaches them from different viewpoints." The Finnish government foresaw no consensus existing "on terms such as cyber attack, cyber defence or cyber conflict/skirmish" and that

[31] Ministry for Foreign Affairs (2020). International law and cyberspace Finland's national positions. https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727.
[32] Ministry for Foreign Affairs (2020). International law and cyberspace Finland's national positions. https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727.
[33] Ministry of Transport and Communications (2003). *National Information Security Strategy*, p. 2, 4-5.

the international legal debate on this complex topic probably is to result in "new legal interpretations on the assessment of cyber incidents at the state level or in international organisations." Presumably, these interpretations were not considered to be legally binding on states but indicating "the objectives which the states participating in the arrangements are prepared to adopt."[34]

In 2016-2017, Finland participated in the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.[35]

The 2016 *Information Security Strategy for Finland* did not take up international law,[36] but the 2019 *Finland's Cyber Security Strategy*, a six-text-pages long document did. The Strategy introduced or refreshed three strategic objectives, international cooperation being one of them. Here, international cooperation reliance "on the existing international law, international treaties and respect for human rights also in the cyber environment" was recognized as well as for the purposes of the maintenance of a universal, free and stable internet, the rule of law, democracy and transparency.[37]

Adherence to international law and the importance of the rules-based international system have been the cornerstones and objectives of the Finnish foreign and security policy for decades, if not for a century. The principle of not allowing Finnish territory to be used for hostilities against third countries has commonly been stated in successive Government Programmes.[38]

[34] Government Resolution (2013). *Finland's Cyber security Strategy* and *The Background dossier of the security committee*, p. 9, 29-30, 33.
[35] UNGA (2017). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Report of the Secretary-General*. A/72/327 (14 August).
[36] Ministry of Transport and Communications (2016). *Information Security Strategy for Finland. The World's Most Trusted Digital Business Environment.*
[37] Secretariat of the Security Committee (2019). *Finland's Cyber Security Strategy.*
[38] For example, Finnish Government (2019). *Programme of Prime Minister Sanna Marin's Government*, section 3.3 "Safe and secure Finland built on the rule of law."

Further examples of implementation

CZECH REPUBLIC *Statement at the OEWG* (2020)	The Czech Republic, in addition to stating its general support for the applicability of international law to cyberspace, has recognized the respect for sovereignty as an independent legal obligation, and listed several types of cyber operations in its territory, which it would consider as a violation of its sovereignty, if attributable to another State.[39] In addition, the Czech Republic has recognized the applicability of the due diligence obligation to the use of ICTs, stating that "States have a legal obligation to act against unlawful and harmful cyber activities emanating from their territory or conducted through cyber infrastructure under their governmental control, provided that they are aware of, or should reasonably be expected to be aware of, such activities." The Czech Republic further stated that in its view, due diligence "is not an obligation of result, but rather an obligation of conduct."[40]
FRANCE *International Law Applied to Operations in Cyberspace* (2020)	France explicitly and in compliance with the due diligence requirement, "ensures that its territory is not used for internationally wrongful acts using ICTs." France also noticed that this "is a customary obligation for States, which must (i) use cyberspace in compliance with international law, and in particular not use proxies to commit acts which, using ICTs, infringe the rights of other States, and (ii) ensure that their territory is not used for such purposes, including by non-state actors." Moreover, France recognizes that the "failure by another State to comply with its due diligence requirement is not a sufficient ground for the use of force against it in the context of cyberattacks carried out from its territory."[41]
KOREA *Reply to UN Secretary-General* (2015)	States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-state actors for unlawful use of ICTs.[42]

[39] "Statement by Mr. Richard Kadlčák Special Envoy for Cyberspace Director of Cybersecurity Department. The UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security." 11 February 2020. https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf.

[40] "Statement by Mr. Richard Kadlčák, Special Envoy for Cyberspace, Director of Cybersecurity Department. The UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security." 13 February 2020. https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20Capacity-building%2013.02.2020.pdf.

[41] Ministry of Defence (2020). International Law Applied to Operations in Cyberspace, para 1.1.1 and 1.2.3. https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

[42] "Developments in the field of information and telecommunications in the context of international security," A/70/172 22 July 2015, reply received from the Republic of Korea, page 12.

CANADA *Submission to the OEWG* (2021)	Canadian submission to the OEWG describes action when a country receives or acquires knowledge its territory being used: The notified State should acknowledge receipt of the request via the relevant national point of contact. When a State has knowledge that its territory or cyber infrastructure is being used for an internationally wrongful act conducted using ICTs that is likely to produce serious adverse consequences in a State, the former State should endeavor to take reasonable, available and practicable measures within its territory and capabilities, consistent with its domestic and international law obligations, to cause the internationally wrongful act to cease, or to mitigate its consequences. A State may gain knowledge of such an act following a notification from an affected State. Such notification must be made in good faith and should be accompanied with supporting information. Supporting information may include sharing possible Indicators of Compromise (IoCs), such as IP address and computers used for malicious ICT acts and malware information. [43]
TRINIDAD AND TOBAGO *National Cyber Security Strategy* (2012)	Trinidad and Tobago *National Cyber Security Strategy* (2012), operational goal 2 recognizes "that awareness at the national level constitutes a pre-requisite for effective protection in cyberspace. Under the strategy, the Government of the Republic of Trinidad and Tobago will assume a leadership role in developing a culture of cyber security. This will necessitate the adoption of a multi-disciplinary and multi-stakeholder approach inclusive of awareness-raising, embedding cyber security in the wider aspects of policy formulation and educating all users of ICT and the Internet on their respective roles in cyberspace.[44]
SWEDEN *Regeringsbeslut, Fö2019/01330* (2020)	Establishing a national cybersecurity centre to coordinate the prevention, detection and management of cyber incidents and function as the national focal point of cybersecurity cooperation, information exchange, advice and exercising as, among others, the Swedish government decided to do (December 2020).[45]
UNITED KINGDOM *Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace*	Building active law enforcement, the UK National Cyber Security Centre Active Cyber Defence (ACD) programme seeks to protect the majority of people in the UK from the majority of the harm, caused by the majority of the attacks, for the majority of the time. This has demonstrated that there

[43] OEWG (2021). "Non-paper listing specific language proposals under agenda item "Rule, norms and principles" from written submissions by delegations". (1 March 2021).
[44] Government of the Republic of Trinidad & Tobago (2012). *National Cyber Security Strategy*, p. 14 and 20. See also, Cyber Security Agency of Singapore (2016). *Singapore's Cybersecurity Strategy*, p. 9, 16-17 and 20; and Ministry of Finance (2018). *Danish Cyber and Information Security Strategy,* p. 21 and 23.
[45] Swedish Government (2020). Regeringsbeslut, Fö2019/01330 (12 December 2020).

(2019)	are targeted interventions that governments can take – alongside the private sector – to improve the digital homeland. [46]
UNITED KINGDOM *National Cyber Security Centre (2021) "Active Cyber Defence"* (2021)	The ACD provides free tools and services, that protect against a range of cyber security threats such as 1.Protective Domain Name Service 2.Web Check 3.Mail Check 4.Host Based Capability 5.Logging Made Easy 6.Vulnerability Disclosure 7.Exercise in a Box 8.Suspicious Email Reporting Service 9.The NCSC Takedown Service 10.MyNCSC.[47]

[46] Foreign and Commonwealth Office (2019). Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015, para 13k.
[47] National Cyber Security Centre (2021). "Active Cyber Defence". https://www.ncsc.gov.uk/section/products-services/active-cyber-defence.

Considerations for practice

- Develop and deepen national understanding of how international law, especially the law of state responsibility and the obligation of due diligence, applies to state uses of ICTs. Coordinate regional views on this and contribute to the international dialogue on how to best apply international law, especially the law of state responsibility and the obligation of due diligence, to state uses of ICTs.

- Create national mechanisms for receiving and handling requests of assistance by other states. Develop regional and international mechanisms for receiving and handling requests of assistance. Promote international cooperation and assistance in case of wrongful ats involving the use of ICTs.

- Take normative steps to prevent non-state actors, including the private sector, from conducting harmful ICT activities to the detriment of third parties, including those located on another state's territory. Engage the private sector in defining permissible and prohibited actions in the use of ICTs. Develop frameworks and tools that help preventing conduct of internationally wrongful acts in your jurisdiction, including relevant certification, best practices, coordination processes.

- Develop situational awareness on key national networks by threat detection and analysis and dedicated authority, such as national cybersecurity centre or government security operations centre (SOC). Enhance situational awareness across government and the private sector by appointing points of contact in key government authorities and establishing information exchange procedures. Participate in relevant regional and global information sharing mechanisms.

- Make a political commitment to uphold international law by issuing a Not Our Behaviour (NOB)[48] pledge on not allowing territory to be used for internationally wrongful acts involving the use of ICTs. Invite other stakeholders to join this commitment and participating in its implementation. Develop regional support to and mechanisms for similar statements and commitment to not allowing territory to be used for internationally wrongful acts involving the use of ICTs.

[48] Cf. voluntary, non-binding No-First-Use -policy or not allowing the deployment of nuclear weapons to country territory or territorial waters known in the nuclear realm.

Recommendation 4: Cooperate to stop crime and 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.

GGE 2021 Guidance:

- This norm reminds States of the importance of international cooperation to addressing the crossborder threats posed by criminal and terrorist use of the Internet and ICTs, including for recruitment, financing, training and incitement purposes, planning and coordinating attacks and promoting their ideas and actions, and other such purposes highlighted in this report. The norm recognizes that progress in responding to these and other such threats involving terrorist and criminal groups and individuals through existing and other measures can contribute to international peace and security.

- Observance of this norm implies the existence of national policies, legislation, structures and mechanisms that facilitate cooperation across borders on technical, law enforcement, legal and diplomatic matters relevant to addressing criminal and terrorist use of ICTs.

- States are encouraged to strengthen and further develop mechanisms that can facilitate exchanges of information and assistance between relevant national, regional and international organizations in order to raise ICT security awareness among States and reduce the operating space for online terrorist and criminal activities. Such mechanisms can strengthen the capacity of relevant organizations and agencies, while building trust between States and reinforcing responsible State behaviour. States are also encouraged to develop appropriate protocols and procedures for collecting, handling and storing online evidence relevant to criminal and terrorist use of ICTs and provide assistance in investigations in a timely manner, ensuring that such actions are taken in accordance with a State's obligations under international law.

- Within the United Nations, a number of dedicated fora, processes and resolutions specifically address the threats posed by terrorist and criminal use of ICTs and the cooperative approaches required to address such threats. Relevant General Assembly resolutions include resolution 65/230 on the Twelfth United Nations Congress on Crime Prevention and Criminal Justice establishing an open-ended intergovernmental expert group (IEG) to conduct a comprehensive study of the problem of cybercrime; resolution 74/173 on promoting technical assistance and capacity-building to strengthen national measures and international cooperation to counter the use of ICTs for criminal purposes, including information sharing; and resolution 74/247 on countering the use of ICTs for criminal purposes.

- States can also use existing processes, initiatives and legal instruments and consider additional procedures or communication channels to facilitate the exchange of information and assistance for addressing criminal and terrorist use of ICTs. In this regard, States are encouraged to continue strengthening efforts underway at the United Nations and at the regional level to respond to criminal and terrorist use of the Internet and ICTs, and develop cooperative partnerships with international organizations, industry actors, academia and civil society to this end.

Elements of implementation

To successfully implement this recommendation, states could consider focusing on national cybercrime laws, law enforcement capacity and mutual assistance mechanisms. The following examples demonstrate how states and organizations have prioritized these elements.

NATIONAL CYBERCRIME LAWS

The Namibian government has drafted a Cybercrime Bill where Chapter 8 “Cybercrime and powers of investigation in criminal matters” would criminalize unauthorized access, unauthorized interference, unlawful devices, system or programs, child pornography, and electronic harassment. The Bill (para 74) would authorize co-operation with foreign authorities in the investigation or prosecution.

Draft Electronic Transactions and Cybercrime Bill (2019)

LAW ENFORCEMENT CAPACITY

As new crimes are developing at an exponential rate, there is a need to carry out proper investigation and prosecute offenders. In this context, a Cybercrime Strategy is required that will enable law enforcement agencies in Mauritius to detect, handle and prosecute cybercriminals and the judiciary to understand this highly technical and complex area whenever cases are brought before Courts.

Mauritius, National Cybercrime Strategy (2017)

MUTUAL ASSISTANCE MECHANISMS

Kenya is a member of the Commonwealth, Harare Scheme and London Scheme relating to Mutual legal assistance in criminal Matters within the Commonwealth. The Office of the Attorney General is the Central Authority for Mutual legal assistance in Kenya. Its functions are to receive, accede and ensure the execution of Mutual Legal Assistance requests.

Office of the Attorney General and Department of Justice Requests for Mutual Legal Assistance in Criminal Matters. Guidance for Authorities Outside of Kenya (2018)

Close-up: MAURITIUS

Steady steps towards more effective combatting of cybercrime

The 2003 Mauritius "Computer Misuse and Cybercrime Act" defines cybercrimes unauthorised access to computer data, access with intent to commit offences, unauthorised access to and interception of computer service, unauthorised modification of computer material (covering also the suppression, modification or impairing of the operation of the computer system), damaging or denying access to computer systems (covering also the degradation, failure, interruption or obstruction of the operation of a computer system), unauthorised disclosure of password, unlawful possession of devices and data, and electronic fraud. The Act sets investigative and procedural rules among other on real time collection of traffic data where there are reasonable grounds on the relevance of such data for investigation and prosecution.[49]

The 2002 Prevention of Terrorism Act had included the "extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property, likely to endanger human life or result in major economic loss" among its description of act of terrorism.[50]

In 2003 Mauritian Parliament also passed the "Mutual Assistance in Criminal and Related Matters Act" mandating "The Central Authority may make a request on behalf of Mauritius to the competent authority of a foreign State, or to an international criminal tribunal, for mutual assistance in any proceedings commenced in Mauritius in relation to a serious offence." Accordingly, a "foreign State may, in relation to a serious offence, and an international criminal tribunal may, in relation to an international criminal tribunal offence, make a request for assistance to the Central Authority in any proceedings commenced in the foreign State or before the international criminal tribunal, as the case may be."[51] Attorney General's Office has published guidance on Mutual Legal Assistance process and procedures.[52]

In the 2014 *National Cyber Security Strategy* the Mauritian government prioritized securing cyberspace and the establishment of "a front line of defense against Cybercrime." Combatting cybercrime was to be "exercised and developed together through international cooperation and the exchange of information." The embedded action plan included the projects of promoting international and regional cooperation on cybercrime, enhancing law enforcement capability on cybersecurity, and assessing legal framework.[53]

The 2017 *Cybercrime Strategy* set the mission to "enhance the Government efforts to tackle cybercrime by providing a more effective law enforcement and criminal justice response" where one of its seven goals covers working with international counterparts to improve cooperation on cybercrime.[54]

---

[49] "Computer Misuse and Cybercrime Act" Act 22 of 2003 (9 August).
[50] "The Prevention of Terrorism Act." Act 2 of 2002 (19 February), Part II (3).
[51] "Mutual Assistance in Criminal and Related Matters Act" Act 35 of 2003 (15 November), Part II (4) and (5).
[52] Attorney General's Office (2021). "Mutual Legal Assistance Process and Procedure in Mauritius." https://attorneygeneral.govmu.org/Documents/MLA/Process%20and%20Procedures%20in%20Mauritius.pdf.
[53] Republic of Mauritius (2014). *National Cyber Security Strategy 2014-2019*, p. 14, 18-19.
[54] Republic of Mauritius (2017). *Cybercrime Strategy 2017-2019*, p. 7.

The *Strategy* emphasised the need of improving the skills and competences of law enforcement and judicial sectors: "As new crimes are developing at an exponential rate, there is a need to carry out proper investigation and prosecute offenders. In this context, a Cybercrime Strategy is required that will enable law enforcement agencies in Mauritius to detect, handle and prosecute cybercriminals and the judiciary to understand this highly technical and complex area whenever cases are brought before Courts."[55]

The *Cybercrime Strategy* acknowledged how "[O]ne commonly experienced difficulty is in making requests for data to other law enforcement agencies or data owners outside the country. This process varies in its success, speed and complexity dependent on the country, or more frequently the company concerned. Many exchanges are facilitated by personal contacts or the reputation of the organisation or individual requesting the data. The success of a request is not always dependent on whether a country has signed an international convention or agreement which indicates it will provide the co-operation sought." Mauritius, a signatory of the *Convention on Cybercrime* ('the Budapest Convention'), emphasises also the harmonisation of legal frameworks in its anti-cybercrime approach. [56]

A key initiative under the *Cybercrime Strategy*, the Mauritian Cybercrime Online Reporting System (MAUCORS) was designed to facilitate secure online cybercrime reporting and develop a better understanding of the cybercrime affecting the Mauritian citizens. It will also provide advice to help in recognising and avoid common types of cybercrime which takes place on social media websites. The information gathered through the system will also help in improving understanding of the scope and cost of, and prevailing trends of cybercrime in Mauritius. MAUCORS has been set up with the collaboration of various stakeholders and is administered by the Computer Emergency Response Team of Mauritius.[57]

In addition, CERT-MU is also affiliated with Forum of Incident Response and Security Teams (FIRST) since May 2012, and Mauritius has contributed to Council of Europe, Cybercrime Office in training programmes in Sri Lanka and Philippines in 2016.[58]

[55] Republic of Mauritius (2017). *Cybercrime Strategy*, p. 6.
[56] Republic of Mauritius (2017). *Cybercrime Strategy 2017-2019*, p. 21-23.
[57] Republic of Mauritius (2021). "The Mauritian Cybercrime Online Reporting System (MAUCORS)", http://maucors.govmu.org/English/Pages/default.aspx. CERT-MU is also affiliated with Forum of Incident Response and Security Teams (FIRST) since May 2012.
[58] *Law Officers' and State Attorneys' Forum*, No. 4 (October 2020), p. 10.

Further examples of implementation

NAMIBIA *Draft Cybercrime Bill* (2015)	Namibian government has drafted a Cybercrime Bill where (para 74) co-operation with foreign authorities in the investigation or prosecution of cybercrimes would be authorized. The draft Bill Chapter 8, "Cybercrime and powers of investigation in criminal matters", would criminalize unauthorized access, unauthorized interference, unlawful devices, system or programs, child pornography, and electronic harassment.[59]
KENYA *Requests for Mutual Legal Assistance in Criminal Matters. Guidance for Authorities Outside of Kenya* **(**2018)	Kenya is a member of the Commonwealth, Harare Scheme and London Scheme relating to Mutual legal assistance in criminal Matters within the Commonwealth. The Office of the Attorney General is the Central Authority for Mutual legal assistance in Kenya. Its functions are to receive, accede and ensure the execution of Mutual Legal Assistance requests. Kenya may allow also requests of interception of tele and other communication also in instances where the "subject is in a third state and the requesting state needs technical assistance of Kenya to intercept." Here, Kenya expects the request to include proof of the subject's presence in a third state and proof that the third state has been informed accordingly.[60]
GREECE *Multilateral assistance treaties* (2018)	As of 2018, Greece had 14 bilateral Mutual Legal Assistance treaties in use as well as ten additional bilateral treaties which are not in use as legal cooperation with those countries is predicated on the Schengen Convention or the European MLA Convention. These treaties contain provisions requiring Greek governmental authorities and their counterparts to provide assistance, establishing certain procedures to be followed in providing assistance, and may also stipulate that a request shall be executed according to the internal laws and procedures of Greece.[61]
SRI LANKA *Statement by the Sri Lanka Delegation* (2019)	Sri Lanka decided to join the Council of Europe Convention on Cybercrime ('Budapest Convention') in 2015 with "strong commitment to harmonize and improve national legislation in accordance with international standards governing cybercrime." National legislative measures taken to addressing evolving cybercrime challenges include the review of the criminal justice measures in the area of child safety online, and an Amendment to the Obscene Publications Ordinance to comprehensively deal with Child Pornography related offences.

[59] Ministry of Information Communications and technology (2019). "draft Electronic Transactions and Cybercrime Bill." https://ictpolicyafrica.org/fr/document/ggel4vdlal?page=1.

[60] Office of the Attorney General and Department of Justice (2018). *Requests for Mutual Legal Assistance in Criminal Matters. Guidance for Authorities Outside of Kenya*, p. 3-4 and 15. https://statelaw.go.ke/wp-content/uploads/2020/11/MLA-GUIDELINES-IN-CRIMINAL-MATTERS-FOR-AUTHORITIES-OUTSIDE-OF-KENYA.pdf.

[61] OECD (2018). *Mutual Legal Assistance: Assessment and revision of the current legal and regulatory framework*. https://www.oecd.org/daf/anti-bribery/OECD-Greece-MLA-Assessment-Legal-Framework-ENG.pdf .In 2018, Greece had bilateral MLA relations with Albania, Armenia, Australia, Canada, China, Cyprus, Egypt, Georgia, Lebanon, Mexico, Russia, Syria, Tunisia, and the United States.

	Sri Lankan government has continued active international participation in enhancing "bilateral, regional and multilateral cooperation to prevent and combat these [transnational organized crime, terrorism, cybercrime] crimes", and reiterated "the need to recognize the importance of international cooperation in criminal matters, including mutual legal assistance and extradition."[62]
G7 *Charlevoix summit* (2018)	At the June 2018 Charlevoix Summit, the Group of Seven (G7) leaders announced to establish a Rapid Reaction Mechanism (RRM) to respond to efforts of foreign actors seeking to "undermine our democratic societies and institutions, our electoral processes, our sovereignty and our security." G7 leaders committed to strengthen coordination to prevent, thwart and respond to malign and evolving threats to G7 democracies by sharing information and threat analysis, and identifying opportunities for coordinated responses. A coordination unit was set up within Global Affairs Canada, which serves as a permanent secretariat to the RRM. The unit is responsible for consolidating and disseminating international lessons learned related to foreign threats to democracy.[63]
EUROPEAN UNION *Council Act of 29 May* **(2000)**	To strengthen their cooperation between judicial, police and customs authorities in criminal matters, the European Union Member States signed a convention on Mutual Assistance in Criminal Matters in 2000. The EU has mutual legal assistance agreements with the United States, Japan, Iceland and Norway.[64]
UNODC *International Cooperation Networks* (2018)	Examples of regional or world-wide judicial cooperation arrangements, include **Judicial Regional Platforms of Sahel and Indian Ocean Commission Countries** established to strengthen international cooperation in criminal matters in the regions of the Sahel and the Indian Ocean. Their main focus is to prevent and combat forms of serious crime, such as organized crime, corruption, drug trafficking or terrorism; the **Commonwealth Network of Contact Persons** facilitating international cooperation in criminal cases between Commonwealth member States, including on mutual legal assistance and extradition, and to provide relevant legal and practical

[62] "Statement by the Sri Lanka Delegation 'Agenda Item 106: Crime Prevention & Criminal Justice; Agenda Item 107: Countering the Use of Information and Communications technologies for criminal purposes and Agenda Item 108: International Drug Control'. 74th Session of the United Nations General Assembly (UNGA), Third Committee (2019). https://www.un.int/srilanka/statements_speeches/statement-delivered-ms-pramuditha-manusinghe-assistant-director-un-human-rights.

[63] Government of Canada (2019). "G7 Rapid Response Mechanism". Government of Canada "G7 Rapid Response Mechanism". https://www.canada.ca/en/democratic-institutions/news/2019/01/g7-rapid-response-mechanism.html; and Government of Canada (2019) "Rapid Response Mechanism Canada - Protecting Democracy". https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/rrm-mrr.aspx?lang=eng.

[64] "Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union." *Official Journal of the European Communities,* C 197/1 (12 July 2000).

information. The Network comprises at least one contact person from each of the jurisdictions of the Commonwealth; the **European Judicial Network** of national contact points for the facilitation of judicial cooperation in criminal matters between the members States of the European Union. National contact points are designated by each member State among central authorities in charge of international judicial cooperation, judicial authorities and other competent authorities with specific responsibilities in the field of international judicial cooperation, both in general and for certain forms of serious crime, such as organized crime, corruption, drug trafficking or terrorism. The Network is composed of more than 300 national contact points throughout the 27 member States, the European Commission and a Secretariat based in The Hague; the **Ibero-American Network of International Legal Cooperation** is a cooperation tool, in civil and criminal matters, made available for all legal agents from the 22 Ibero-American countries and the Supreme Court of Puerto Rico. The Central Authorities are those established in instruments of International Law in which the countries belonging to the Ibero-American Community are a part of regarding judicial cooperation in criminal and civil matters.[65]

[65] United Nations Office on Drugs and Crime (2021). "International Cooperation Networks." https://www.unodc.org/unodc/en/legal-tools/international-cooperation-networks.html.

Considerations for practice

- Adopt general cybercrime legislation and specific according to cybercrime levels, risks and areas. Review and update national legislation periodically, considering national lessons learned and based on best practices identified in regional and global cooperation on combatting cybercrime.

- Establish cybercrime investigate function within national police and security services. Educate investigative and judicial personnel in cybercrime and terrorist use of ICT matters. Conduct bilateral, regional or global information sharing training and exercises.

- Develop cyber situational awareness function in national security and criminal systems. Promote interagency reporting and intelligence fusion capability. Participate in bilateral, regional or global information and intelligence sharing mechanisms, *e.g.* through Interpol Cybercrime Collaboration Services.

- Study different regional and global regimes and mechanisms for combatting cybercrime. Join regional or global cybercrime regimes that best serve national requirements and needs. Contribute to improving regional or global cybercrime normative or operational frameworks.

- Determine key relationships with other states and stakeholders to enhance national cybercrime combatting capacity. Establish Mutual Legal Assistance Treaties (MLAT) with countries assessed relevant for countering terrorist and criminal use of ICTs. Inform and promote global efforts in countering terrorist and criminal use of ICTs.

Recommendation 5: Respect human rights and 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.

GGE 2021 Guidance:

- This norm reminds States to respect and protect human rights and fundamental freedoms, both online and offline in accordance with their respective obligations. Requiring special attention in this regard is the right to freedom of expression including the freedom to seek, receive and impart information regardless of frontiers and through any media, and other relevant provisions provided for in the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and as set out in the Universal Declaration of Human Rights. Observance of this norm can also contribute to promoting non-discrimination and narrowing the digital divide, including with regard to gender.

- Adoption of the resolutions referenced in this norm and others that have since been adopted is an acknowledgement of new challenges and dilemmas that have emerged around the use of ICTs by States and the corresponding need to address them. State practices such as arbitrary or unlawful mass surveillance may have particularly negative impacts on the exercise and enjoyment of human rights, particularly the right to privacy.

- In implementing this norm, States should consider specific guidance contained in the cited resolutions. They should also take note of new resolutions adopted since the 2015 GGE report and contribute to new resolutions that may need to be advanced in light of ongoing developments.

- Efforts by States to promote respect for and observance of human rights and ensure the responsible and secure use of ICTs should be complementary, mutually reinforcing and interdependent endeavours. Such an approach promotes an open, secure, stable, accessible and peaceful ICT environment. It can also contribute to the achievement of the Sustainable Development Goals (SDGs).

- While recognizing the importance of technological innovation to all States, new and emerging technologies may also have important human rights and ICT security implications. To address this, States may consider investing in and advancing technical and legal measures to guide the development and use of ICTs in a manner that is more inclusive and accessible and does not negatively impact members of individual communities or groups.

- The Group notes that within the United Nations a number of dedicated fora specifically address human rights issues. In addition, it acknowledges that a variety of stakeholders contribute in different ways to the protection and promotion of human rights and fundamental freedoms online and offline. Engaging these voices in policy-making processes relevant to ICT security can support efforts for the promotion, protection and enjoyment of human rights online and help clarify and minimize potential negative impacts of policies on people, including those in vulnerable situations.

Elements of implementation

To successfully implement this recommendation, states could consider focusing on commitment to privacy and freedom of information, national legislation in this field and adequate oversight mechanisms. The following examples demonstrate how states and organizations have prioritized these elements.

COMMITMENT TO PRIVACY AND FREEDOM OF INFORMATION

The Nepalese National Information and Communication Technology Policy highlights the importance of underlines the need to protect fundamental rights of the citizens in building confidence and security. Nepal Telecommunication Authority has issued guidelines on online child safety.

Nepal Telecommunications Authority draft National Cybersecurity Policy (August 2016).
Nepal Telecommunications Authority Guidelines issued by the Authority as per the Telecommunication Act 1997 (2019)

NATIONAL LEGISLATION

The Philippines 2012 "Data Privacy Act" acknowledges that "the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth." The Act also reiterates the protection of journalists and their sources, created the National Privacy Commission as an independent body to monitor and ensure compliance of the country with international standards set for data protection.

National Privacy Commission Republic Act 10173 – Data Privacy Act of 2012

ADEQUATE OVERSIGHT MECHANISMS

Cote D'Ivoire's administrative measures taken to safeguard the respect of human rights include establishing Parliamentary oversight and control mechanisms. Parliament intelligence committee and Ombudsman can be mandated to inspect law enforcement and the security and intelligence agencies' investigatory, including surveillance and intelligence practices.

Republique de Cote D'Ivoire D'orientation de la societe de l'information en Cote D'Ivoire (2017)

Close-up: ICELAND

Deep national commitment to rights and freedoms online

The fight for human rights and women's empowerment, peace and disarmament have high priority in Iceland's foreign policy. These are values that the Icelandic Government wants to emphasize in international cooperation, values that the Government has also taken on as an international commitment.[66]

Iceland's national security policy is based on the commitments provided for in the Charter of the United Nations. It is guided by the basic values of:

- Democracy
- Respect for the rule of law and international law
- Humanitarianism and protection of human rights
- Equal rights for all
- Sustainable development, and
- Disarmament and peaceful resolution of conflicts.

The fundamental premise of the national security policy is Iceland's status as a sparsely populated island nation that has neither the resources nor the desire to maintain an army.

Comprehensive security and defence is sought and provided through active cooperation, both with other countries and within international organisations. This principle covers also cyber security which is pursued through continued development of Iceland's internal capacity and cooperation with other countries.[67]

Human rights are one of the cornerstones of Iceland's foreign policy. In accordance with the UN Charter Articles 55 and, the member states have committed themselves to measures conducive to acknowledging human rights and fundamental freedom without any discrimination.

Iceland works towards the protection and furtherance of human rights in the world, primarily within the relevant international organizations. This is achieved for example through

- participation in ensuring the implementation of current international agreements regarding human rights
- through participation in the drafting of new international agreements and participation in the making of resolutions
- exchange of opinions and work at grassroots level where measures and policies of the international community are formed
- calling the attention of the international community to any lack of respect for human rights, occasions of systematic violations of human rights are, and
- finding ways to combat such violations.

[66] Government of Iceland (2021). "National Security." https://www.government.is/topics/foreign-affairs/national-security/.
[67] *National Security Policy for Iceland* (2016). Parliamentary document 1166 — Case no. 327. no. 26/145. https://www.government.is/media/utanrikisraduneyti-media/media/Varnarmal/National-Security-Policy-ENS.pdf. Also, Government of Iceland (2021) "National Security." https://www.government.is/topics/foreign-affairs/national-security/.

Iceland regards human rights are universal and concern everyone, everywhere, regardless of time and space. They are an integral part of international relations, not the private matter of each state. This becomes obvious as the interaction between human rights, sustainable development, peace and security has been widely comprehended. Iceland's human rights policy is integrated into all areas of foreign policy. Iceland has ratified all major international conventions and agreements on human rights and encourages other states to do the same and advocates for the implementation of said conventions and agreements.[68]

The *Icelandic Cyber Security Strategy* (2015) envisions Iceland to have an Internet culture that is sound, promotes human rights, protects the individual and respects freedom of action to support economic prosperity and development. The *Strategy* prioritises the inclusion of security and privacy considerations from the outset in the design process, that is, to *security by design* and *privacy by design.* Moreover, cyber security, and its human rights aspects, must form a part of computer-related studies at all levels of the educational system.[69]

In its overview of the Icelandic state of affairs, Freedom House concluded that

> "Iceland remained the world's best protector of internet freedom during the coverage period [mid 2019-mid 2020]. Users in this island country enjoy near-universal connectivity, minimal restrictions on online content, and strong protections for their rights online. The coverage period saw Parliament pass a long-awaited whistleblower protection law, a part of the Icelandic Modern Media Initiative. However, other legislative elements of the initiative continued to be stalled. The government's response to the COVID-19 pandemic involved the rollout of a voluntary contact tracing app that was hailed for giving users control over their personal data."[70]

In a joint Nordic-Baltic statement at the UN discussion on the Secretary General's "Call to Action for Human Rights", Iceland's government concluded, that

> *In our view and based on our experience, there is no way around human rights if we are to achieve just, inclusive, democratic and – importantly – more resilient societies*.[71]

[68] Government of Iceland (2021). "Human Rights in Foreign Policy." https://www.government.is/topics/foreign-affairs/human-rights-in-foreign-policy/.
[69] Ministry of the Interior (2015). *Icelandic National Cyber Security Strategy 2015-2026. Plan of Action 2015-2018,* p. 3, 5
[70] Freedom House (2021) "Iceland." https://freedomhouse.org/country/iceland/freedom-net/2020.
[71] Government of Iceland (2021). "Statement on behalf of the Nordic-Baltic countries on the Secretary General's Call to Action for Human Rights." https://www.government.is/diplomatic-missions/permanent-mission-of-iceland-to-the-united-nations/statements/statement/2021/02/24/Statement-on-behalf-of-the-Nordic-Baltic-countries-on-the-Secretary-Generals-Call-to-Action-for-Human-Rights-/.

Further examples of implementation

COSTA RICA *Estrategia Nacional de Ciberseguridad de Costa Rica* (2017)	The Costa Rican Government acknowledges the values enshrined in the universal declaration of human rights. It regards the guaranteeing of the respect of human rights and privacy fundamental. Particular attention is paid to access to ICTs. The measures resulting from the 2017 *Estrategia Nacional de Ciberseguridad* must at all times safeguard the human rights and privacy of information of the country's inhabitants. In fact, the Strategy has been developed taking into account the need to balance the protection of all inhabitants and respect for basic and fundamental human rights, with the need to implement measures to keep them safe online. This includes respect for freedom of expression, freedom of speech, the right to privacy, freedom of opinion, and freedom of association.[72]
NEPAL *National Information and Communication Technology Policy* (2018)	The Nepalese National Information and Communication Technology Policy highlights the importance of underlines the need to protect fundamental rights of the citizens in building confidence and security.[73] Nepal's Telecommunication Authority has issued guidelines on online child safety.[74]
MALTA *National Cyber Security Strategy* (2016)	The Maltese National Cyber Security Strategy includes the rule of law as a guiding principle: "The approach on cyber security shall respect and promote fundamental rights and freedoms as chartered within European Union and national legislation. All measures shall comply with the principles of necessity, proportionality and legality, with appropriate safeguards to ensure accountability and redress."[75]
LAOS *Speech of Minister of Posts and Telecommunications* (2016)	Lao Minister of Posts and Telecommunications, Dr. Thansamay Kommasith aligned human development and information and telecommunication technology, including cybersecurity. He underlined the significance of ICTs for the Lao government commitment to developing and improving the living standards of its people by transforming the country from landlocked to land linked nation. "We will make ICT work to support our development and empowerment." Moreover, he expressed the Lao commitment to fulfilling its international commitments and "willingness to contribute to cyber security dialogue with

[72] Ministerio de Ciencia, Tecnología y Telecomunicaciones (2017). *Estrategia Nacional de Ciberseguridad de Costa Rica,* p. 8, 35.
[73] Nepal Telecommunications Authority (2018). draft *National Cybersecurity Policy* (August 2016). See also, for example, Burkina Faso (2010) *Plan national de cybersecurite de Burkina Faso*, p. 7.
[74] Nepal Telecommunications Authority (2019). Guidelines issued by the Authority as per the Telecommunication Act 1997. https://nta.gov.np/en/guidelines-issued-by-the-authority-as-per-the-telecommunication-act-1997-a-d/.
[75] Ministry for Competitiveness and Digital, Maritime and Services Economy (2016). *National Cyber Security Strategy*, p. 12.

	our experience and create new norms of responsible state behaviour".[76] This statement aligns well with Lao government and the Ministry earlier being pleased with the ASEAN ICT master plan 2020 where the first key area, in particular, stresses the importance of an accessible and inclusive digital economy.[77]
COTE D'IVOIRE *D'orientation de la societe de l'information en Cote D'Ivoire* (2017)	The Ivory Coast parliament recognized and affirmed that access to the Internet and to electronic communication networks is a fundamental human right and a universal good. The State also committed to guarantee universal access to telecommunication/ICT services.[78] Administrative measures taken to safeguard the respect of human rights is to establish Parliamentary oversight and control mechanisms. Parliament intelligence committee and Ombudsman can be mandated to inspect law enforcement and the security and intelligence agencies' investigatory, including surveillance and intelligence practices.[79]
UNITED STATES *Reaction to the cyber-attack against Sony Pictures Entertainment* (2014)	In reaction to the cyber-attack against Sony Pictures Entertainment in 2014, Homeland Security Secretary Johnson noted that "the cyber-attack against Sony Pictures Entertainment was not just an attack against a company and its employees. It was also an attack on our freedom of expression and way of life.[80] The United States condemned North Korea for the cyber-attack: "These actions are a brazen attempt by an isolated regime to suppress free speech and stifle the creative expression of artists beyond the borders of its own country".[81]
NORWAY *Reply to UN Secretary-General* (2017)	Universal human rights also apply in the cyberdomain. The same rights that individuals have offline must also be protected online, in particular freedom of expression, including the freedom to seek, receive and impart information and the right to privacy.[82]

[76] Thansamay Kommasith (2016). "Opening remarks". ICT for Peace Foundation Cambodia-Laos-Miyanmar-Vietnam Workshop on International Cyber Security Policy and Diplomacy for CLMV Countries. Vientianne, (31 October).
[77] *ASEAN Ministerial Conference on Cyber Security*, 10-12 October 2016, Singapore.
[78] Republique de Cote D'Ivoire (2017). *D'orientation de la societe de l'information en Cote D'Ivoire,* Article 3. No. 2017-803 (7 Decembre).
[79] On the European Union and its Member States oversight mechanisms, see European Union Agency for Fundamental Rights (2017). *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*. Vienna, European Union Agency for Fundamental Rights.
[80] United States Department of Homeland Security (2014). "Jeh C. Johnson, 'Statement by Secretary Johnson on Cyber Attack on Sony Pictures Entertainment'." (19 December). https://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment.
[81] United States Department of State (2014). "John Kerry, 'Condemning Cyber-Attack by North Korea." (19 December). https://2009-2017.state.gov/secretary/remarks/2014/12/235444.htm.
[82] Developments in the field of information and telecommunications in the context of international security, A/72/315 11 August 2017 submission by Norway, p. 26.

FRANCE *Reaction to the cyber-attack against TV5Monde* (2015)	French Prime Minister Manuel Valls called the attack against TV5Monde 'an unacceptable insult to freedom of information and expression'.[83]
SWEDEN *Reply to UN Secretary-General* (2014)	Sweden was one of the initiators of the Freedom Online Coalition (FOC), a coalition of governments committed to advancing human rights online. Since its inception in 2011 the coalition has grown from 15 to 23 member countries. FOC conducts yearly high-level meetings and issues joint statements and declarations. In close cooperation with a core group of states, Sweden initiated the UN Human Rights Council resolution in 2012, which affirmed that the same rights that individuals have offline must be protected online. The resolution was adopted by consensus and co-sponsored by 87 countries, giving it significant cross-regional backing.[84]
ARGENTINA *Reply to UN Secretary-General* (2019)	With respect to the protection of personal data, Argentina was one of the first countries of the region to have a regulatory framework for the protection of personal data, through the adoption of Act No. 25.326. Argentina has acceded to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. On 1 June 2019, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and its Additional Protocol, will enter into force in the Argentine Republic.[85]
FREEDOM ONLINE COALITION	The Freedom Online Coalition is a group of governments who have committed to work together to support Internet freedom and protect fundamental human rights – free expression, association, assembly, and privacy online – worldwide. The Coalition members coordinate their diplomatic efforts, share information on violations of human rights online and work together to voice concern over measures that curtail human rights online. The Coalition also collaborates by issuing joint statements, by sharing policy approaches to complex issues, exchanging views on strategy, and planning participation in relevant forums. Additionally, the Coalition provides a platform for multistakeholder engagement, which is also recognized in its founding declaration. This work has included the shaping of global norms on human rights online through joint statements in relevant international forums and

[83] Angelique Chrisafis and Samuel Gibbs (2015). 'French Media Groups to Hold Emergency Meeting after Isis Cyber-Attack,' *The Guardian* (9 April). https://www.theguardian.com/world/2015/apr/09/french-tv-network-tv5monde-hijacked-by-pro-isis-hackers.
[84] Developments in the field of information and telecommunications in the context of international security, A/69/112/Add.1 18 September 2014, reply received from Sweden, page 6. See also UN Human Right Council Resolutions 20/8, 26/13, 32/13 and 38/7.
[85] Developments in the field of information and telecommunications in the context of international security
Report of the Secretary-General, A/74/120, 24 June 2019. Replies received from governments: Argentina, page 3.

resolutions and raising awareness of priority issue areas and their implications for human rights online through public workshops/events.[86]

UN HUMAN RIGHTS RAPPORTEUR'
Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2010)

UN Human Rights Rapporteur report on the promotion and protection of human rights and fundamental freedoms while countering terrorism, offers best practices applicable also in the field of telecommunications and information. For example, on the legal mandates and powers of intelligence services, the practices include:

Practice 2. The mandates of intelligence services are narrowly and precisely defined in a publicly available law. Mandates are strictly limited to protecting legitimate national security interests as outlined in publicly available legislation or national security policies, and identify the threats to national security that intelligence services are tasked to address. If terrorism is included among these threats, it is defined in narrow and precise terms.

Practice 3. The powers and competences of intelligence services are clearly and exhaustively defined in national law. They are required to use these powers exclusively for the purposes for which they were given. In particular, any powers given to intelligence services for the purposes of counter-terrorism must be used exclusively for these purposes.

Practice 4. All intelligence services are constituted through, and operate under, publicly available laws that comply with the Constitution and international human rights law. Intelligence services can only undertake or be instructed to undertake activities that are prescribed by and in accordance with national law. The use of subsidiary regulations that are not publicly available is strictly limited, and such regulations are both authorized by and remain within the parameters of publicly available laws. Regulations that are not made public do not serve as the basis for any activities that restrict human rights.[87]

[86] Freedom Online Coalition (2021). "Aims and priorities." https://freedomonlinecoalition.com/about-us/about/
[87] United Nations General Assembly (2010). Human Rights Council Agenda item 3 Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin." A/HRC/16/51 (22 December 2010).

Considerations for practice

- Affirm political and legal commitment to the respect of human rights online, including access to the Internet. Adopt cybersecurity, data protection and privacy legislation where human rights commitments and obligations are recognized, promoted and protected against any violations. Work regionally and internationally to champion the respect of human rights, tolerance and indiscrimination.

- Promote national processes for implementation of human rights and fundamental freedoms online, including by awareness, dedicated programs and due process. Establish national authorities with a mandate for oversight, administrative and public guidance and ombudsman functions regarding privacy and other human rights issues. Support enhancement and refinement of export controls of malicious ICT tools and techniques which may easily be used to deliberately violate human rights.

- Determine and debate appropriate balance between human rights and fundamental freedoms and national security. Establish judicial, administrative and/or parliamentary domestic oversight mechanisms on State surveillance of communications, their interception and the collection of personal data. Periodically review and revise national security legislation, including surveillance, monitoring, collection and use of data from the perspective of protection of privacy and basic rights and freedoms.

- Conduct awareness and public education campaigns on rights, freedoms and protections online and to combat hatred and all forms of discrimination. Enhance awareness through supporting civil society and school and academic programs and activities on human rights and fundamental freedoms online. Conduct national human rights impact assessments to support policy and action reviews, exchange and develop views on respecting and protecting human rights online.

- Align digital development and cybersecurity policies with Sustainable Development Goals to ensure effective and mindful use of public resources for the good of the people and their rights and freedom.

- Strengthen human rights considerations in national arms control and export regimes for example by stricter end-user certification

Recommendation 6: 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.

GGE 2021 Guidance:

- With regard to this norm, ICT activity that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public can have cascading domestic, regional and global effects. It poses an elevated risk of harm to the population, and can be escalatory, possibly leading to conflict.

- This norm also points to the fundamental importance of critical infrastructure as a national asset since these infrastructures form the backbone of a society's vital functions, services and activities. If these were to be significantly impaired or damaged, the human costs as well as the impact on a State's economy, development, political and social functioning and national security could be substantial.

- As noted in norm 13 (g), States should take appropriate measures to protect their critical infrastructure. In this regard, each State determines which infrastructures or sectors it deems critical within its jurisdiction, in accordance with national priorities and methods of categorization of critical infrastructure.

- The COVID-19 pandemic heightened awareness of the critical importance of protecting health care and medical infrastructure and facilities, including through the implementation of the norms addressing critical infrastructure (such as this norm and norms (g) and (h)). Other examples of critical infrastructure sectors that provide essential services to the public can include energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes. Critical infrastructure may also refer to those infrastructures that provide services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet. Such infrastructure can be critical to international trade, financial markets, global transport, communications, health or humanitarian action. Highlighting these infrastructures as examples by no means precludes States from designating other infrastructures as critical, nor does it condone malicious activity against categories of infrastructures that are not specified above.

- To support implementation of the norm, in addition to consideration of the factors outlined above, States are encouraged to put in place relevant policy and legislative measures at the national level to ensure that ICT activities conducted or supported by a State and that may

impact the critical infrastructure of or the delivery of essential public services in another State are consistent with this norm, used in accordance with their international legal obligations, and subject to comprehensive review and oversight.

Elements of implementation

To successfully implement this recommendation, states could consider focusing on condemning malicious activity, adhering to their international obligations and transparency about military cyber capabilities. The following examples demonstrate how states and organizations have prioritized these elements.

CONDEMNING MALICIOUS ACTIVITY

We stand united as we face this unprecedented coronavirus pandemic. We condemn destabilising and malicious cyber activities directed against those whose work is critical to the response against the pandemic, including healthcare services, hospitals and research institutes.

Statement by the North Atlantic Council concerning malicious cyber activities (2020)

ADHERENCE TO INTERNATIONAL LAW

States reaffirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. In this regard, States were called upon to avoid and refrain from taking any measures not in accordance with international law, and in particular the Charter of the United Nations.

OEWG Final Substantive Report (2021), para 34

TRANSPARENCY ABOUT CAPABILITIES

When developing cyber military capabilities, the United States has been transparent on the purpose and direction of military cyberspace operations through publishing ministerial (department) and joint doctrines and field manuals and other publicly available steering documents.

E.g. Department of Defense (2011) Department of Defense Strategy for Operating in Cyberspace; Joint Chiefs of Staff (1998) Joint Doctrine for Information Operations (JP 3-13); and (2013 and 2018) Cyberspace Operations (JP 3-12)

Close-up: COSTA RICA

Pacific and human-centric security

Since ability to conduct malicious or harmful cyber operations against any target requires for any state considerable set of organizational, technical and work force resources, deliberate lack of such power projection capabilities speaks of restraint.

After a civil war, Costa Rica abolished her armed forces in 1948. For over seventy years Costa Rican "history and record on the environment, human rights, and advocacy for the peaceful settlement of disputes" and the subsequent practice of strong regional and global cooperation have been heralded.[88] Today Costa Rica, celebrating her bicentennial independence, is ranked among the top twenty most peaceful countries in the world.[89]

Costa Rican government is together with is Latin American and Caribbean partners committed to international cooperation, multilateralism and the conformity with international law, including international human rights law. The government is urging states to "refrain from enacting and unilaterally apply economic, financial or commercial measures that are not compatible with the international law and the Charter of the United Nations and that prevent the full achievement of development economic and social, particularly in developing countries."[90]

On the other hand, organized and transnational crime, mainly illegal drug trade and trafficking, could foster cybercrime and breed illegal organized non-state cyber in Costa Rica. Bilateral and regional security cooperation and national cyber security policy, strategy and capability development in the field of law enforcement, judicial capacity and incident management seek to mitigate such a risk.

The 218 Costa Rican security strategy, *Sembremos Seguridad,* prioritizes and targets crimes, and social risks and other factors that affect citizens, identifies criminal structures and articulates inter-institutional and institutional capacities. It is of public and national interest, that the strategies, lines of action, programs and projects that derive from its implementation, promote peaceful coexistence, the strengthening of the citizen security and national welfare as well as the creation of safe spaces and the promotion of social peace.[91]

Accordingly with the country's pacific policy orientation, security cooperation with, for example, the United States focuses on law enforcement and human security issues. It covers the areas of transnational organized crime and rising domestic violence, and the US provides Costa Rican law enforcement and domestic security authorities with equipment, training, and capacity building to transform its air service, its Coast Guard, and its border and immigration services. The bilateral partnership extents to building investigative, prosecutorial, and corrections capability for Costa Rica's

[88] U.S. Embassy in Costa Rica (2021). "Policy and history". https://cr.usembassy.gov/our-relationship/policy-history/; United Nations Secretary-General (2018). "Secretary-General's Press Conference with Costa Rican President Carlos Alvarado Quesada". https://www.un.org/sg/en/content/sg/press-encounter/2018-07-16/secretary-generals-press-conference-costa-rican-president.
[89] Institute for Economics & Peace (2020). Global Peace Index 2020: Measuring Peace in a Complex World, Appendix C, "Ongoing Domestic and International Conflict domain."
[90] *Cuarta Reunión del Foro de los Países de América Latina y el Caribe sobre el Desarrollo Sostenible*. "Proyecto de conclusions y recomendaciones acordadas sobre el desarrolo sostenible." (12 March 2021), para 42, 47.
[91] "Oficializa y declara de interés público y nacional la Estrategia Integral de Prevención para la Seguridad Pública 'Sembremos Seguridad'". *La Gaceta* no. 41242-SP. 4 September 2018, Article 2 and 3.

public security and judicial organizations. To enhance economy and business opportunities, sound economic reforms, adoption of best practices, removal of economic barriers, infrastructure improvements, and the rule of law are considered suitable approaches for Costa Rica.[92]

Costa Rica's Estrategia Nacional de Ciberseguridad (2017) recognizing cyber challenges affecting all the inhabitants of the world and the need of "a concert of nations", is anchored in national development plans and the principles of

- Human centric security recognizing the centrality of the Universal Declaration of Human Rights as well as privacy
- Coordination and co-responsibility of multi-stakeholders
- International cooperation.[93]

The key objectives of the Strategy focus on the development of national, by default, civilian cyber safety and security capabilities.

Costa Rica is to participate in international cooperation through mutual assistance and collaboration in criminal, technical, educational matters and the development of security measures to address cybersecurity related issues. To respond quickly and diligently to risks and vulnerabilities, collaboration and cooperation between the various national and international actors is required. Costa Rican government, in line with its general pacific and collaborative orientation, acknowledges the importance of global dialogue on cyberspace shaping the nation's future.[94]

[92] U.S. Department of State (2018). *Integrated Country Strategy. Costa Rica,* p. 2 and 9.
[93] Ministerio de Ciencia, Tecnología y Telecomunicaciones (2017). *Estrategia Nacional de Ciberseguridad de Costa Rica,*p. 8-9, 11.
[94] Ministerio de Ciencia, Tecnología y Telecomunicaciones (2017). *Estrategia Nacional de Ciberseguridad de Costa Rica,*p. 47.

Further examples of implementation

CANADA *Statement in the OEWG* (2020)	Canada, among others, emphasised the national prerogative of deciding what infrastructure, function or service is considered critical. Canada wants to ensure that any such definition does not implicitly condone malicious activity against other categories of infrastructure not defined as critical.[95]
CHINA *Statement in the OEWG* (2020)	China explicitly emphasises state sovereignty and state commitments not to use ICTs counter to international peace and security.[96]
THE NETHERLANDS *Statement in the OEWG* (2021)	The Netherlands stressed the general availability or integrity of the public core of the Internet as a guidance to implement the recommendation.[97]
AUSTRALIA *Attribution of a Pattern of Malicious Cyber Activity to Russia* (2018)	In response to ransomware attack dubbed Bad Rabbit, Australia stated that "the International Community – including Russia – has agreed that international law and norms of responsible state behaviour apply in cyberspace. By embarking on a pattern of malicious cyber behaviour, Russia has shown a total disregard for the agreements it helped to negotiate."[98]
EUROPEAN UNION *Council Conclusions on Malicious Cyber Activities* (2018)	The EU has stressed, with reference to the WannaCry cyber-attack, that the use of ICTs for malicious purposes is unacceptable.[99]
NEW ZEALAND AND OTHERS *New Zealand Condemns Malicious Cyber Activity Against Georgia*	In response to the cyber-attacks against Georgian … in 2019, New Zealand states: 'These malicious cyber activities serve no legitimate interest. They were designed to interfere in Georgia's political and economic freedom.

[95] OEWG (2021). Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions by delegations" (1 March 2021), https://front.un-arm.org/wp-content/uploads/2021/03/2021-03-01-non-paper-rules-norms-and-principles.pdf.
[96] OEWG (2021). Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions by delegations" (1 March 2021), https://front.un-arm.org/wp-content/uploads/2021/03/2021-03-01-non-paper-rules-norms-and-principles.pdf.
[97] OEWG (2021). Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions by delegations" (1 March 2021), https://front.un-arm.org/wp-content/uploads/2021/03/2021-03-01-non-paper-rules-norms-and-principles.pdf.
[98] Prime Minister of Australia (2018). 'Attribution of a Pattern of Malicious Cyber Activity to Russia.' https://www.pm.gov.au/media/attribution-pattern-malicious-cyber-activity-russia.
[99] Council of the European Union (2018). "Council Conclusions on Malicious Cyber Activities." 7925/18 (16 April).

(2020)	Activities which seek to undermine democratic processes are unacceptable. New Zealand urges all states to abide by the framework of responsible state behaviour online.'[100] Statements were also made by the United Kingdom,[101] the US,[102] Australia,[103] Canada,[104] Ukraine,[105] Estonia,[106] Poland,[107] the Czech Republic,[108] the Netherlands,[109] Denmark,[110] Lithuania,[111] Norway,[112,] Latvia[113] and Finland[114].
OEWG	According to the "Zero draft report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security" (19 January 2021) countries seemed to be of agreeing "that the COVID-19 pandemic accentuated the importance of

[100] Government Communications Security Bureau (2018). "New Zealand Condemns Malicious Cyber Activity Against Georgia". https://www.scoop.co.nz/stories/WO2002/S00123/new-zealand-condemns-malicious-cyber-activity-against-georgia.htm.
[101] Foreign & Commonwealth Office (2020). "Dominic Raab, 'UK Condemns Russia's GRU over Georgia Cyber-Attacks,'" (20 February). https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.
[102] United States Department of State (2020). "Michael R. Pompeo, 'The United States Condemns Russian Cyber Attack Against the Country of Georgia,'" (20 February). https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/.
[103] Australian Ministry for Foreign Affairs (2020). "Marise Payne, 'Attribution of Malicious Cyber Activity in Georgia by Russian Military Intelligence.'" (21 February). https://www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-malicious-cyber-activity-georgia-russian-military-intelligence.
[104] Global Affairs Canada (2020). "Canada condemns Russia's malicious cyber-activity targeting Georgia." https://www.canada.ca/en/global-affairs/news/2020/02/canada-condemns-russias-malicious-cyber-activity-targeting-georgia.html.
[105] Ministry of Foreign Affairs of Ukraine (2020). "Comment of the Ministry of Foreign Affairs of Ukraine on Cyberattacks committed by the Russian Federation against Georgia-" (20 February). https://mfa.gov.ua/news/komentar-mzs-ukrayini-shchodo-kiberatak-vchinenih-rosijskoyu-federaciyeyu-proti-gruziyi.
[106] Ministry of Foreign Affairs (2020) "Urmas Reinsalu, 'Statement of the Foreign Minister of the Republic of Estonia." (20 February). https://vm.ee/en/news/statement-foreign-minister-republic-estonia-urmas-reinsalu.
[107] 'Statement of the Polish MFA on Cyberattacks against Georgia,' Ministry of Foreign Affairs Republic of Poland, 20 February 2020, https://www.gov.pl/web/diplomacy/statement-of-the-polish-mfa-on-cyberattacks-against-georgia.
[108] Ministry of Foreign Affairs of the Czech Republic (2020), '1/2 @CzechMFA Condemns Cyberattacks on Georgia from October 28, 2019 […],' Twitter, 20 February, https://twitter.com/CzechMFA/status/1230491060150964230?s=20.
[109] The Ministry of Foreign Affairs of the Netherlands (2020).'The Netherlands Considers Russia's GRU Responsible for Cyber Attacks against Georgia: Diplomatic Statement.' (20 February). https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2020/02/20/the-netherlands-considers-russia's-gru-responsible-for-cyber-attacks-against-georgia.
[110] The Ministry of Foreign Affairs of Denmark (2020), 'UK & US Attribute the Serious and Disruptive Cyber-Attacks against Georgia to Russia's Military Intelligence Service (GRU) […],' Twitter (20 February), https://twitter.com/DanishMFA/status/1230483524123320322?s=20.
[111] The Ministry of Foreign Affairs of the Republic of Lithuania (2020). 'Recalling the 2019 October Disruptive Cyber-Attack against Georgia Media and Governmental Webpages, Lithuania Strongly Reiterates […],' Twitter, 20 February 2020, https://twitter.com/LT_MFA_Stratcom/status/1230485445798219777?s=20.
[112] The Royal Norwegian Ministry of Foreign Affairs (2020). 'We Share Concerns about Cyber Operations in Georgia […],' Twitter, 20 February 2020, https://twitter.com/NorwayMFA/status/1230487577502855169?s=20.
[113] The Ministry of Foreign Affairs of Latvia (2020).'Latvia Condemns Cyber-Attack against Georgia,' The Ministry of Foreign Affairs of the Republic of Latvia (21 February). https://www.mfa.gov.lv/en/news/latest-news/65504-latvia-condemns-cyber-attack-against-georgia.
[114] Ministry for Foreign Affairs of Finland (2020). 'Finland FM @Haavisto Condemns the cyber-Attack against Georgia [...],' Twitter, 21 February, https://twitter.com/ulkoministerio/status/1230824890296655872?lang=en.

	protecting healthcare infrastructure including medical services and facilities as part of the norms addressing critical infrastructure."[115]
NATO	The North Atlantic Treaty Organisation Member-States similarly have condemned cyber activities against healthcare services: "We stand united as we face this unprecedented coronavirus pandemic. We condemn destabilising and malicious cyber activities directed against those whose work is critical to the response against the pandemic, including healthcare services, hospitals and research institutes."[116]
G7 *Declaration on responsible states behaviour in cyberspace* (2017)	Concerned of the destabilizing effects on international peace and security caused by escalation and retaliation in cyberspace and malicious cyber activity impairing the use and operation of critical infrastructure that provide services to the public, G7 governments encourage all states to engage in law-abiding, norm-respecting and confidence-building behaviour in their use of ICT. They also call on states to publicly explain their views on international law to give rise to more settled expectations of state behavior.

[115] "Zero draft report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security", para 55. Draft as of 19 January 2021 with Russian amendments, https://front.un-arm.org/wp-content/uploads/2021/02/RF-OEWG-zero-draft-report-with-the-Russian-amendments-ENG.pdf.
[116] North Atlantic Council (2020). *Statement by the North Atlantic Council concerning malicious cyber activities*. https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en.

Considerations for practice

- Promote education and studies in international law and how it applies to state uses of ICTs. Develop clear national understanding on how to apply international law in cyberspace. Share national views on how to apply international law in cyberspace.

- To express political and practical commitment, issue deferring Not-Our-Behaviour (NOB)[117] pledge on not conducting or knowingly supporting ICT activity contrary to international law. Invite other stakeholders to join this commitment and participating in its implementation. Invite regional support to and develop collaborative mechanisms for similar statements and commitment on not conducting or knowingly supporting ICT activity contrary to international law.

- Determine which infrastructures, sectors or services are deemed critical, in accordance with national priorities and methods of categorization of critical infrastructure. Create awareness and acknowledgment of responsible behaviour in cyberspace, also among non-state actors, especially the private sector and CI operators.

- Develop a mentality of prevention and de-escalation among all national stakeholders. Criminalize targeting and harming other states critical infrastructure providing services to public. Issue operational rules of engagements which prohibits targeting other states critical infrastructure providing services to public.

- Condemn ICT activity that intentionally damages critical infrastructure. Join countries and other stakeholders in condemning and imposing consequences to ICT activity that intentionally damages critical infrastructure. Promote responsible state behaviour and application of international law with emphasis on preventing ICT activity that intentionally damages critical infrastructure.

[117] Cf. voluntary, non-binding No-First-Use -policy or not allowing the deployment of nuclear weapons to country territory or territorial waters known in the nuclear realm.

Recommendation 7: Protect 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.

GGE 2021 Guidance:

- This norm reaffirms the commitment of all States to protect critical infrastructure under their jurisdiction from ICT threats and the importance of international cooperation in this regard.

- A State's designation of an infrastructure or sector as critical can be helpful for protecting said infrastructure or sector. In addition to determining the infrastructures or sectors of infrastructure it deems critical, each State determines the structural, technical, organizational, legislative and regulatory measures necessary to protect their critical infrastructure and restore functionality if an incident occurs. General Assembly resolution 58/199 on the Creation of a global culture of cybersecurity and the protection of critical information infrastructures and its accompanying annex[118] highlights actions that States can take at the national level to that end.

- Some States serve as hosts of infrastructures that provide services regionally or internationally. ICT threats to such infrastructure could have destabilizing effects. States in such arrangements could 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.

- Encouraging measures to ensure the safety and security of ICT products throughout their lifecycle or to classify ICT incidents in terms of their scale and seriousness would also contribute to the objective of this norm.

[118] United Nations General Assembly (2004). *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*. A/RES/58/199 (30 January).

Elements of implementation

To successfully implement this recommendation, states could consider focusing on national critical infrastructure protection plans, critical infrastructure risk assessment and cooperation with sectors and operators. The following examples demonstrate how states and organizations have prioritized these elements.

NATIONAL CI PROTECTION PLAN

The Russian Federation identifies critical information infrastructure protection as one of the main thrusts of the information security. It comprises enhancing the protection of the critical information infrastructure and reliability of its functioning, developing mechanisms of identification and prevention of information security threats and elimination of their effects, as well as enhancing the protection of citizens and territories from the effects of emergencies caused by information and technical impacts on the objects of critical information infrastructure.

Doctrine of Information Security of the Russian Federation (5 December 2016)

CI RISK ASSESSMENT

The United Arab Emirates outlines the key stages of applying risk reduction to critical information infrastructures by

- Conducting baseline sectorial assessments
- Performing sectorial and national risk assessments
- Defining sectorial plans
- Monitoring the implementation of the plans.

The United Arab Emirates National Cyber Security Plan (2019)

COOPERATION WITH SECTORS AND OPERATORS

Singapore guides Critical Information Infrastructure owners that operate OT systems and other enterprises facing similar OT threats and vulnerabilities, such as oil and gas sector manufacturing plants, semiconductor factories, and pharmaceutical companies, and the OT cybersecurity industry, including equipment manufacturers, system integrators and penetration testers.

Singapore's Operational Technology Cybersecurity Masterplan (2019)

Close-up: SINGAPORE

Determination to secure national infrastructure

The first Singapore *Infocomm Security Masterplan* (ISMP) (2005-2007) was launched to coordinate cybersecurity efforts across the Government. Its key priority was the build-up basic capabilities within the public sector to mitigate and respond to cyber threats. After these initial steps were sufficiently implemented, the (second) 2008 *Infocomm Security Masterplan* (2008-2012) turned main efforts to the security of Singapore's critical information infrastructure (CII).[119] Singapore government noted country's success in this area "be determined by its ability to provide a secure and trusted infocomm environment." For that purpose, the first 'strategic thrust' was set to harden national infocomm infrastructure with the aim of enhancing the resilience of Singapore underlying foundation to combat cyber threats.[120] The (third) *National Cyber Security Masterplan 2018* (2013) expanded the scope to take into consideration businesses and individuals. Its mission was described to enhance "cyber security capabilities in four focal areas – Government, Critical Infocomm Infrastructure, Businesses and Individuals."[121] After this gradual development, Singapore felt competent to issue her first consolidating cyber security strategy in 2016.

As Prime Minister Lee Hsien Loong has confirmed,

> *The Cybersecurity Strategy outlines Singapore's vision, goals and priorities. We are determined to protect essential services from cyber threats, and to create a secure cyberspace for businesses and communities.*

Singapore's Cyber Security Strategy of 2016 outlined the six measures under its first pillar, "Building a Resilient Infrastructure" as follows:

> First, we will enhance our CII Protection Programme to establish robust and systematic cyber risk management processes across all critical sectors. Second, we will improve our sectors' response and recovery plans to breaches. We will mount multi-sector cybersecurity exercises to test cooperation across multiple sectors and address inter-dependencies during major cyber-attacks. We will also expand and beef up national resources such as the National Cyber Incident Response Team (NCIRT) and the National Cyber Security Centre (NCSC). Next, we will introduce the Cybersecurity Act to give the Cyber Security Agency of Singapore (CSA) greater powers to secure our CIIs. Finally, as threats to government networks will continue to grow, we will expand efforts to secure government systems and networks, so as to protect citizens' and official data.[122]

With the establishment of the Cyber Security Agency of Singapore (CSA) in 2015, national cybersecurity was brought under a single agency (the Prime Minister's Office). The CSA is dedicated to the protection of CIIs and essential services. CSA is also empowered to develop and enforce cybersecurity regulations, policies, and practices as well as the coordination of cybersecurity efforts across government, industry, academia, businesses and the people sector, as well as internationally.

---

[119] Cyber Security Agency of Singapore (2016). *Singapore's Cybersecurity Strategy,* p. 7.
[120] Info-communications Development Authority (2008). *Infocomm Security Masterplan 2*, p. 1-2.
[121] Info-communications Development Authority (2013). *National CyberSecurity Masterplan*, p. 9.
[122] *Singapore's Cyber Security Strategy*, p. 4, 8-15.

In 2018 Singapore issued the *Cybersecurity Act* where the Commissioner of Cybersecurity has the legal mandate to identify and designate CII and to regulate owners of CII with regard to the cybersecurity of the CII. Furthermore, the Commissioner was authorized to establish cybersecurity codes of practice and standards of performance for implementation by owners of critical information infrastructure.[123] Under the Act (section 15(1) (a)) the owner of a CII must cause a cybersecurity audit of the compliance of the CII with the Act and applicable codes of practice and standards of performance. The cybersecurity audit must be carried out at least once every two years (or at such higher frequency as may be directed by the Commissioner of Cybersecurity in any particular case), and to be carried out by an auditor approved or appointed by the Commissioner. For this purpose, the CSA issued *Guidelines for Auditing Critical Information Infrastructure.*[124]

Moreover, in 2019 the government issued *Singapore's Operational Technology Cybersecurity Masterplan.* Aiming to enhance the security and resilience of Singapore's essential service sectors, the Masterplan seeks to improve cross-sector response to mitigate cyber threats in the OT environment, and strengthen partnerships with industry and stakeholders. Under the OT cybersecurity Masterplan, the OT Information Sharing and Analysis Centre (OT-ISAC) facilitates secured information exchange between the OT owners, vendors and operators, both locally and globally, to advance security and ensure operational resiliency. The Masterplan applies to both CII owners that operate OT systems, as well as other enterprises that face the same OT threats and similar vulnerabilities, among others manufacturing plants in the oil and gas sector, semiconductor factories, and pharmaceutical companies. The focus of the Masterplan is on industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and programable logic controllers (PLC)[125].[126]

How profoundly Singapore acknowledges the value of international cooperation, regional, ASEAN, endeavours and global normative frameworks in critical information infrastructure protection, is signified in the following ministerial speech at the ASEAN Ministerial Conference on Cybersecurity:

> *Like many other ASEAN States, we are concerned also with safeguarding CII within our jurisdiction. CIIs constitute national assets which form the backbone of our societies' most vital functions, services and activities. Many cities within ASEAN serve as key hubs for services spanning the banking and finance, telecommunications, aviation and maritime sectors. Thus, the impact of a cyberattack on a national CII may not be confined to that country alone, but also felt in other parts of the region and even the world. Many member states recognise the risks and are taking proactive steps to protect their national CIIs. These efforts are in line with the UNGGE norms that we have agreed upon. Beyond protecting national CIIs, ASEAN can do more to strengthen regional cyber resilience by safeguarding CIIs with cross-border impact, such as common cloud and banking systems. In fact, the significance of*

[123] *Cybersecurity Act 2018.* Government Gazette no. 9. Part 2, 5e and f.
[124] Cyber Security Agency of Singapore (2020). *Guidelines for Auditing Critical Information Infrastructure.*
[125] Control systems are computer based used by many infrastructures and industries to monitor and control sensitive processes and physical functions. Control systems usually collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment. (Robert Radvanovsky & Jacob Brodsky (eds.) (2016) *Handbook of SCADA/Control Systems Security*. CRC Press, p. 3-4)
[126] Cyber Security Agency of Singapore (2019). *Singapore's Operational Technology Cybersecurity Masterplan*, p. 1, 3, 16, 22-27, 29-41.

the Cloud has been heightened because of the pandemic and the response from industry. The need to secure these CIIs cannot be overstated.[127]

[127] "Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity." *ASEAN Ministerial Conference on Cybersecurity 2020*. https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2020.

Further examples of implementation

DOMINICAN REPUBLIC
national cybersecurity strategy for 2018-2021
(2018)

The Dominican Republic national cybersecurity strategy for 2018-2021 defines within the strategic pillar of national critical infrastructure and state information infrastructure protection the four specific objectives of:

1. Identifying of national critical infrastructure and information infrastructure relevant for the state and conducting a risk analysis
2. Developing and implementing a plan to strengthen national critical infrastructure and state information infrastructure as well as for the services which support them against cyber threats
3. Improving inter-sectorial and inter-institutional coordination for protection of information systems and national critical infrastructure and state information infrastructure and the private sector
4. Developing a cyber incident response plan for national critical infrastructure and state information infrastructure and the private sector.[128]

ESTONIA
Cybersecurity Act
(2018)

As a European Union Member State, Estonia has implemented mandatory cyber safety and security measures on both critical and essential services.

The Emergency Act of 2017 defines a vital service as a service that has an overwhelming impact on the functioning of society and the interruption of which is an immediate threat to the life or health of people or to the operation of another vital service or service of general interest.[129]

The Cybersecurity Act of 2018 icludes requirements for the maintenance of network and information systems essential for the functioning of society and state and local authorities' network and information systems, liability and supervision as well as the bases for the prevention and resolution of cyber incidents.[130]

THE RUSSIAN FEDERATION
Doctrine of Information Security of the Russian Federation
(2016)

The Russian Federation identifies critical information infrastructure protection as one of the main thrusts of the information security. It comprises enhancing the protection of the critical information infrastructure and reliability of its functioning, developing mechanisms of identification and prevention of information security threats and elimination of their effects, as well as enhancing the protection of citizens and territories from the effects of emergencies caused by information and technical impacts on the objects of critical information infrastructure.[131]

---

[128] Dominican Republic (2018). *Estrategia Nacional de Ciberseguridad 2018-2021*, p. 6-8.
[129] Estonian Parliament (2017). "Emergency Act." (8 February). https://www.riigiteataja.ee/en/eli/ee/505012018004/consolide.
[130] Estonian Parliament (2018). "Cybersecurity Act." (9 May), para 1. https://www.riigiteataja.ee/en/eli/523052018003/consolide.
[131] The Ministry of Foreign Affairs of the Russian Federation (2016). *Doctrine of Information Security of the Russian Federation,* para 23c.

IRELAND
National Cyber Security Strategy 2019-2024
(2019)

The Irish National Cyber Security Strategy 2019-2024 has defined specific measures to control and evaluate the implementation of the Strategy. Below is one example of measures in critical infrastructure protection with two action items.[132]

Measure 6: The existing information sharing groups operated by the National Cyber Security Centre will be further developed, with the existing Threat Sharing Group being broadened to include a wider range of critical national infrastructure.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Expand the current Threat Sharing Group (TSG) representatives to include CNI, with new Terms of Reference.	Q2 2020	NCSC	AGS, DF, CNI
2	Refine existing arrangements with the UK on information sharing and incident response, with particular reference to North-South critical infrastructure protection.	Q4 2020	NCSC	OEP, CPNI UK

SERBIA
Reply to UN Secretary-General
(2016)

The Law defined the ICT systems of special importance in Serbia, which means that operators have to undertake the adequate technical and organizational measures in order to ensure the security of the ICT systems. These systems are: 1) ICT systems of public bodies, 2) ICT systems where the sensitive personal data is handled, 3) ICT systems in the areas of public interest (energy, transport, gas, banking, health care and other). They are recognized as important, because they are used by operators to provide vital services, perform business activities and store personal data. The operators have to undertake the protection measures defined in the law and by-laws, in accordance with the national and international standards. The operators of ICT systems of special importance are obliged to inform competent authority on incidents which may have significant impact on violation of information security.[133]

ARGENTINA
Reply to UN Secretary-General
(2019)

Argentina has a National Critical Information and Cybersecurity Infrastructure Programme established by Resolution 580/2011 of the Executive Office of the Cabinet of Ministers. The Programme is designed to define and protect public and private sector strategic and critical infrastructure, as well as that of international organizations, manage all information on reports of security incidents and direct potential solutions in an organized and consolidated way, among other objectives. In this context, a protocol has been established for situations where public agencies are highly vulnerable to digital security risks, and which provides for linkages to the private sector. Work is currently under way to develop a norm that will establish a definition of "critical information infrastructure", criteria for determining whether infrastructure is critical, and categorize the infrastructure of various sectors.[134]

[132] Government of Ireland (2019). *National Cyber Security Strategy 2019-2024*, p. 30.
[133] Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General, A/71/172, 16 July 2016. Replies received from governments: Serbia, page 1-2.
[134] Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General, A/74/120, 24 June 2019. Replies received from governments: Argentina, p. 3.

UNITED ARAB EMIRATES *National Cyber Security Plan* (2019)	The United Arab Emirates 2019 National Cyber Security Plan (NCSP) approximates application programs to protect critical information infrastructure as • Identification of programs for the protection of critical information infrastructure • Develop a general national approach to identify critical information infrastructures • Identification of electronic security requirements for critical information infrastructures • and compliance areas • Defining the main roles and tasks of the main stakeholders • Develop a general approach to enhance cooperation and communication between critical areas.[135] The NCSP outlines the key stages of applying risk reduction to critical information infrastructures by • Conducting baseline sectorial assessments • Performing sectorial and national risk assessments • Defining sectorial plans • Monitoring the implementation of the plans.[136]
GEORGIA *Reply to UN Secretary-General* (2014)	Penetration testing has been conducted at several government agencies as a part of target hardening of critical information systems. All tests have been conducted on a basis of formal agreements and the results have been duly reported to the beneficiary institutions.[137]

[135] UAE Telecommunications Regulatory Authority (2019). *National Cyber Security Plan*, p. 10-11.
[136] UAE Telecommunications Regulatory Authority (2019). *National Cyber Security Plan*, p. 10-11. The NCSP functions as a detailed action plan for the 2019 *National Cyber Security Strategy* (UAE Telecommunications Regulatory Authority (2019) *National Cybersecurity Strategy).*
[137] Developments in the field of information and telecommunications in the context of international security, A/69/112 30 June 2014, reply received from Georgia, p. 9.

Considerations for practice

- Develop a national cybersecurity strategy and an action plan with critical infrastructure protection (CIP) being one of the prioritized objectives or lines of action. Devise a comprehensive critical infrastructure protection implementation plan which covers information and operational technologies and processes. Promote bilateral, sub-regional or regional critical infrastructure planning in areas of *e.g.* energy distribution, information infrastructure or sea fare.

- Determine which infrastructures, sectors or services are deemed critical and prioritized, in accordance with national priorities and methods of categorization of critical infrastructure. Adopt legislation which assists the defined critical infrastructure operators in preparing CIP contingency and management plan as well as organize regular training and exercises in their field, sector or service. Require regular audits and assessments to detect CI vulnerabilities and address threats in critical infrastructures, sectors or services.

- Adopt legislation which allows public-private partnership including participation and exchange of information in CIP. Include the private sector to national CIP planning and implementation by *e.g.* establishing obligatory and voluntary venues, mechanisms and procedures of contribution. Incorporate national and societal CIP considerations in public and private industrial IT/OT and infrastructural planning.

- Promote cooperation with CI operators and the private sector and academia to enhance CI threat assessment and design programs and preparedness for preventing ICT threats. Develop CI monitoring, assessment, reporting and other incident management mechanisms and capabilities, including forensic ones, in cooperation with the private sector. Participate in bilateral, regional and global efforts of CI protection, lessons learned and best practices.

- Develop a national CIP training and exercise regime. Participate in regional and global training and exercises focused on CI and CII. Incorporate CI and CII training and exercises to other national security and preparedness training and exercises.

Recommendation 8: 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.

GGE 2021 Guidance:

- This norm reminds States that international cooperation, dialogue, and due regard for the sovereignty of all States are central to responding to requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. The norm is particularly important when dealing with those acts that have the potential to threaten international peace and security.

- Upon receiving a request for assistance, States should offer any assistance they have the capacity and resources to provide, and that is reasonably available and practicable in the circumstances. A State may choose to seek assistance bilaterally, or through regional or international arrangements. States may also seek the services of the private sector to assist in responding to requests for assistance.

- Having the necessary national structures and mechanisms in place to detect and mitigate ICT incidents with the potential to threaten international peace and security enables the effective implementation of this norm. Such mechanisms complement existing mechanisms for day-to-day ICT incident management and resolution. For example, a State wishing to request assistance from another State would benefit from knowing who to contact and the appropriate communication channel to use. A State receiving a request for assistance needs to determine, in as transparent and timely a fashion as possible and respecting the urgency and sensitivity of the request, whether it has the capabilities, capacity and resources to provide the assistance requested. States from which the assistance is requested are not expected to ensure a particular result or outcome.

- Common and transparent processes and procedures for requesting assistance from another State and for responding to requests for assistance can facilitate the cooperation described by this norm. In this regard, common templates for requesting assistance and responding to such requests can ensure that the State seeking assistance provides as complete and accurate information as possible to the State from which it seeks the assistance, thereby facilitating cooperation and timeliness of response. Such templates could be developed voluntarily at the bilateral, multilateral or regional level. A common template for responding to assistance requests could include elements that acknowledge receipt of the request and, if assistance is possible, an indication of the timeframe, nature, scope and terms of the assistance that could be provided.

- Where the malicious activity is emanating from a particular State's territory, its offer to provide the requested assistance and the undertaking of such assistance may help minimize damage, avoid misperceptions, reduce the risk of escalation and help restore trust. Engaging in cooperative mechanisms that define the means and mode of crisis communications and of incident management and resolution can strengthen observance of this norm.

Elements of implementation

To successfully implement this recommendation, states could consider focusing on points od contact, assistance frameworks and rapid reaction capabilities. The following examples demonstrate how states and organizations have prioritized these elements.

POINTS OF CONTACT

To facilitate communication between national cybersecurity authorities the Organization for Security and Cooperation (OSCE), and the Association of Southeast Asian Nations (ASEAN) have established regional points of contact schemes.

ASEAN Critical Information Infrastructure Protection Framework (2020)

ASSISTANCE FRAMEWORKS

Many computer emergency response teams are cooperating within FIRST, Forum of Incident Response and Security Teams framework. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

Forum of Incident Response and Security Teams (2021)

RAPID REACTION TEAMS

A group of EU Member States have established a Cyber Rapid Response Teams (CRRTs) mechanism. The mechanism will allow the Member States to help each other to ensure a higher level of cyber resilience and collectively respond to cyber incidents.

PESCO (2019) "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security"

Close-up: THE UNITED STATES AND RUSSIA

Bilateral CBMs

The Russian Federation and the United States have a history of political disagreements and accusations of the use of ICTs against each other. The two countries have put a bilateral effort into promoting practical cooperation between their respective authorities. In 2013 a working group was established to that end within the U.S.-Russia Bilateral Presidential Commission as a part of US-Russian cybersecurity confidence-building measures (CBMs).[138]

True to the nature and purpose of CBMs, enhancing transparency, confidence and stability and reducing the possibility that a misunderstood cyber incident could create instability or a crisis, the working group addressed a broad range of issues of mutual interest on threats to and in the use of ICTs in the context of international security.

A key component of the discussion concerned the implementation of the bilateral confidence building measures signed by Presidents B. Obama and V. Putin during a Group of Eight *Lough Erne Summit* on June 17, 2013. These bilateral CBMs were intended to promote transparency and enhance strategic stability by reducing tensions caused by threats to and in the use of ICTs:[139]

Links between Computer Emergency Response Teams
To facilitate the regular exchange of practical technical information on cybersecurity risks to critical systems, we are arranging for the sharing of threat indicators between the U.S. Computer Emergency Readiness Team (US-CERT), located in the Department of Homeland Security, and its counterpart in Russia. On a continuing basis, these two authorities will exchange technical information about malware or other malicious indicators, appearing to originate from each other's territory, to aid in proactive mitigation of threats. This kind of exchange helps expand the volume of technical cybersecurity information available to our countries, improving our ability to protect our critical networks.

Exchange of Notifications through the Nuclear Risk Reduction Centers
To prevent crises, the United States and Russia also recognize the need for secure and reliable lines of communication to make formal inquiries about cybersecurity incidents of national concern. In this spirit, we have decided to use the longstanding Nuclear Risk Reduction Center (NRRC) links established in 1987 between the United States and the former Soviet Union to build confidence between our two nations through information exchange, employing their around-the-clock staffing at the Department of State in Washington, D.C., and the Ministry of Defense in Moscow. As part of the expanded NRRC role in bilateral and multilateral security and confidence building arrangements, this new use of the system allows us to quickly and reliably make inquiries of one another's competent authorities to reduce the possibility of misperception and escalation from ICT security incidents.

---

[138] The White House (2013). "Fact sheet: U.S.-Russian Cooperation on Information and Communications Technology Security" (June 17), also Department of State (2017). "U.S.-Russian Bilateral Presidential Commission: Working Groups/Cyber", https://2009-2017.state.gov/p/eur/ci/rs/usrussiabilat/c60405.htm. For time being, the United States has temporarily suspended several projects and meetings planned under the auspices of the U.S.-Russia Bilateral Presidential Commission.
[139] The White House (2013). *Joint Statement on the Inaugural Meeting of the U.S.-Russia Bilateral Presidential Commission Working Group on Threats to and in the Use of Information and Communication Technologies (ICTs) in the Context of International Security*. (22 November). https://obamawhitehouse.archives.gov/the-press-office/2013/11/22/joint-statement-inaugural-meeting-us-russia-bilateral-presidential-commi.

White House-Kremlin Direct Communications Line
Finally, the White House and the Kremlin have authorized a direct secure voice communications line between the U.S. Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council, should there be a need to directly manage a crisis situation arising from an ICT security incident. This direct line will be seamlessly integrated into the existing Direct Secure Communication System ("hotline") that both governments already maintain, ensuring that our leaders are prepared to manage the full range of national security crises we face internationally.

"Taken together, [the CBMs] represent important progress by our two nations to build confidence and strengthen our relations in cyberspace; expand our shared understanding of threats appearing to emanate from each other's territory; and prevent unnecessary escalation of ICT security incidents."[140]

The implementation of this CERT-focussed measure includes the sharing of threat indicators, exchange technical information about malware or other malicious indicators appearing to originate from each other's territory, to aid in proactive mitigation of threats. In specific, the US-RU CBM discussion of communication between the respective CERTs refers to the territory of origin issue.[141]

At a follow-up meeting in November 2013, the Working Group on Threats to and in the Use of ICTs in the Context of International Security reaffirmed that these bilateral CBMs are intended to promote transparency and enhance strategic stability by reducing tensions caused by threats to and in the use of ICTs.[142] Russia and the United States have further discussed the implementation of the bilateral CBMs, and ways to promote regional CBMs in venues such as the OSCE and the ASEAN Regional Forum.

In 2019, Andrei Krutskikh, Ambassador at Large of the Russian Federation, Special Presidential Representative for international cooperation in information security confirmed the usefulness of this mechanism: "Six years ago, in 2013, we managed to reach agreement on establishing a direct line of communication between Russia and the U.S. in the event of cyber incidents. Basically, the system was modelled on a similar mechanism that had been in place during the Cold War for dealing with traditional military incidents and enables a prompt information exchange at all levels from institutional to political."[143]

[140] The White House (2013). "Fact sheet: U.S.-Russian Cooperation on Information and Communications Technology Security" (17 June).
[141] The White House (2013). "Fact sheet: U.S.-Russian Cooperation on Information and Communications Technology Security" (17 June).
[142] The White House (2013). "Joint Statement on the Inaugural Meeting of the U.S.-Russia Bilateral Presidential Commission Working Group on Threats to and in the Use of Information and Communication Technologies (ICTs) in the Context of International Security."
[143] Embassy of the Russian Federation in the United Republic of Tanzania (2019). "Article by Andrei Krutskikh, Ambassador at Large of the Russian Federation, Special Presidential Representative for international cooperation in information security, published in the Kommersant business daily on March 27, 2019." https://tanzania.mid.ru/web/tanzania-en/publications-on-russia/-/asset_publisher/CLelxjfwPHrC/content/article-by-andrei-krutskikh-ambassador-at-large-of-the-russian-federation-special-presidential-representative-for-international-cooperation-in-informa?inheritRedirect=false&redirect=https://tanzania.mid.ru:443/web/tanzania-en/publications-on-russia%3Fp_p_id%3D101_INSTANCE_CLelxjfwPHrC%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-2%26p_p_col_count%3D1.

Further examples of implementation

UKRAINE *Cooperation to mitigate a cyber incident* (2016)	When a cyber-attack caused power outages and blackouts in 103 cities and towns across Ukraine, leaving more than 200,000 customers in several areas without power for up to six hours,[144,145] the Ukrainian government closely collaborated with the United States. An interagency team was created to investigate the incident in Ukraine. The participating parties were the US Computer Emergency Readiness Team (US-CERT), the National Cybersecurity and Communications Integration Center (NCCIC)/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Department of Energy, Federal Bureau of Investigation, and the North American Electric Reliability Corporation.[146] US Department of Homeland Security issued an alert and detailed the mitigation measures.[147]
ESTONIA *Cooperation to mitigate a cyber incident* (2007)	When cyber-attacks resulted in downtime of Estonian government websites, online banking and online media outlets, threatening the security of an entire nation[148], Estonian government requested and received assistance from several governments and organizations. For instance, CERT-EE worked with the Finnish, German, Israeli, and Slovenian colleagues to restore normal network operations. NATO CERTs provided additional assistance, while the EU's European Network and Information Security Agency (ENISA) offered expert technical assessments of the developing situation.[149]
JAPAN *Reply to UN Secretary-General* (2019)	Japan will work to build confidence among States in order to prevent the occurrence of unforeseen circumstances and the deterioration of the situation caused by cyberattacks. Due to the anonymity and secrecy of cyberattacks, there are risks that cyberattacks could unintentionally increase tensions among States and worsen the situation. To prevent such accidental and unnecessary confrontations, it is important to build up international communication channels during peaceful times in preparation for the occurrence of incidents that extend beyond national borders. It is also

[144] 'Analysis of the Threat to Electric Grid Operations,' *Dragos*, 12 June 2017, https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf.
[145] 'Russian govt. behind attack on Ukraine power grid: U.S. officials,' *Homeland Security Newswire*, 16 February 2016, http://www.homelandsecuritynewswire.com/dr20160216-russian-govt-behind-attack-on-ukraine-power-grid-u-s-officials.
[146] 'Cybersecurity and Infrastructure Security Agency (2016). "Cyber-Attack Against Ukrainian Critical Infrastructure." (25 February). https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01.
[147] 'Cyber-Attack Against Ukrainian Critical Infrastructure.'
[148] Vincent Joubert, 'Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?,' *Research Division – NATO Defense College, Rome* (2012), https://www.files.ethz.ch/isn/143191/rp_76.pdf; Davis, 'Hackers Take Down the Most Wired Country in Europe.'
[149] Kertu Ruus (2008). 'Cyber War I: Estonia Attacked from Russia,' *European Affairs* 9:1 (Winter/Spring 2008): Columbia International Affairs Online; Stephen Herzog (2011). 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses,' *Journal of Strategic Security*, Vol. 4, No. 2, Strategic Security in the Cyber Age (Summer 2011).

	necessary to increase transparency and build confidence between States through the proactive information exchange and policy dialogues in bilateral and multilateral consultations. The Government will also cooperate with other States to consider a mechanism for coordinating issues regarding cyberspace.[150]
GEORGIA AND LITHUANIA *Declaration of Intent on Cyber Security Cooperation* (2019)	In 2019, the Ministry of Defence of Georgian and the Ministry of National Defence of Lithuania signed a Declaration of Intent on Cyber Security Cooperation. "Considering the Hybrid threats and challenges the modern world is facing on, we are totally positive with defining Cyber Sphere as a new operational dimension. Our critical infrastructure might be at risk of cyber attacks. Therefore, it is necessary to strengthen the national efforts, deepen cooperation and share experience of our international partners and hold international exercises in order to prevent such incidents". The declaration covers cooperation, experience sharing, planning and execution of joint Cyber Exercises as well as the concentration of mutual efforts in case of national and international cyber incidents.[151]
OAS Critical Infrastructure Protection in Latin America and the Caribbean (2018)	As a region, we have made great strides and continue to improve effective cooperation in the area of hemispheric security. Our focus now must turn to thinking more strategically about critical infrastructure and critical information protection in the region and to providing the necessary incentives and environment to foster good practices in this area.[152] However, before any partnership can be embarked upon, countries need to recognize that this is an area of policy where it is in everyone's interest, and vital, to cooperate.[153]
ASEAN *Critical Information Infrastructure Protection framework* (2018)	The ASEAN has under its Critical Information Infrastructure Protection framework initiated the improvement of regional cyber emergency responses and collaboration.[154]
EUROPEAN UNION *PESCO*	Under the European Union "Permanent Structured Cooperation" (PESCO) framework, a group of EU Member States have established a Cyber Rapid

[150] Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General, A/74/120, 24 June 2019. Replies received from governments: Japan, p. 31.
[151] https://mod.gov.ge/en/news/read/7179/georgia-and-lithuania-to-strengthen-cooperation-in-cyber-security
[152] OAS (2018). Critical Infrastructure Protection in Latin America and the Caribbean. https://www.oas.org/es/sms/cicte/cipreport.pdf, p.9.
[153] OAS (2018). Critical Infrastructure Protection in Latin America and the Caribbean. https://www.oas.org/es/sms/cicte/cipreport.pdf, p. 16.
[154] ASEAN (2018). *Critical Information Infrastructure Protection framework.* https://www.slideshare.net/ETDAofficialRegist/asean-critical-information-infrastructure-protection-framework.

(2019)	Response Teams (CRRTs) mechanism.[155] The mechanism will allow the Member States to help each other to ensure a higher level of cyber resilience and collectively respond to cyber incidents. CRRTs can be used to assist other Member States, EU Institutions, CSDP operations as well as partners. CRRTs will be equipped with a commonly developed deployable cyber toolkits designed to detect, recognise and mitigate cyber threats. Teams are able to assist with training, vulnerability assessments and other requested support. Cyber Rapid Response Teams operate by pooling participating Member States experts. All participating Member States have signed the Declaration of Intent, Political and Legal Memos detailing decision making process have been issued. The first common exercise has been organized, and CRRT has operational capability.[156]
FIRST	Many state computer emergency response teams together with private sector teams are cooperating within FIRST, Forum of Incident Response and Security Teams framework. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.[157]

[155] The participant countries are Croatia, Estonia, Lithuania, the Netherlands, Poland and Romania.
[156] PESCO (2019). "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security." https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/.
[157] Forum of Incident Response and Security Teams (2021). "FIRST is the global Forum of Incident Response and Security Teams". https://www.first.org/.

Considerations for practice

- Develop a national cybersecurity strategy and an action plan with emphasis on public information security (CIA), critical infrastructure protection and combatting cybercrime. Expand national cybersecurity strategy to include in possible detection, verification and response the private sector and societal functions. Incorporate bilateral and regional assistance and capacity building in national cybersecurity policy.

- Establish a national cyber incident management system with 24/7 operational capacity and special emphasis on the need to coordinate and respond to requests by other states or their authorities. Facilitate establishment of sectorial, including industrial cyber incident management system, including forensic capacity with special emphasis on the need to coordinate and respond to requests by other states or their authorities. Support other countries efforts to establish and develop their national cyber incident management systems with special emphasis on the need to coordinate and respond to requests by other states or their authorities

- Develop a deployable rapid reaction and assistance mechanism. Exchange best practices in reaction and response. Promote creating commonly accepted classifications and lexicons to facilitate international response and assistance.

- Determine relevant national points of contact. Establish regional points of contact schemes, liaison and exchanges of information to increase international interoperability. Participate in regional and international exchange and assistance mechanisms.

- Conduct national drills and exercises for response and assistance. Engage in bilateral, regional and global CIP exercises where the deployability and quality of assistance mechanisms can be tested, evaluated and developed. Promote best practices of assistance in international dialogues and processes.

Recommendation 9: 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.

GGE 2021 Guidance:

- This norm recognizes the need to promote end user confidence and trust in an ICT environment that is open, secure, stable, accessible and peaceful. Ensuring the integrity of the ICT supply chain and the security of ICT products, and preventing the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions are increasingly critical in that regard, as well as to international security, and digital and broader economic development.

- Global ICT supply chains are extensive, increasingly complex and interdependent, and involve many different parties. Reasonable steps to promote openness and ensure the integrity, stability and security of the supply chain can include:

    (a) Putting in place at the national level comprehensive, transparent, objective and impartial frameworks and mechanisms for supply chain risk management, consistent with a State's international obligations. Such frameworks may include risk assessments that take into account a variety of factors, including the benefits and risks of new technologies.
    (b) Establishing policies and programmes to objectively promote the adoption of good practices by suppliers and vendors of ICT equipment and systems in order to build international confidence in the integrity and security of ICT products and services, enhance quality and promote choice.
    (c) Increased attention in national policy and in dialogue with States and relevant actors at the United Nations and other fora 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.
    (d) Cooperative measures such as exchanges of good practices at the bilateral, regional and multilateral levels on supply chain risk management; developing and implementing globally interoperable common rules and standards for supply chain security; and other approaches aimed at decreasing supply chain vulnerabilities.

- To prevent the development and proliferation of malicious ICT tools and techniques and the use of harmful hidden functions, including backdoors, States can consider putting in place at the national level:

    (a) 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 lifecycle of ICT products. To this end, States may also consider establishing independent and impartial certification processes.
    (b) Legislative and other safeguards that enhance the protection of data and privacy.
    (c) Measures that prohibit the introduction of harmful hidden functions and the exploitation of vulnerabilities in ICT products that may compromise the confidentiality, integrity and availability of systems and networks, including in critical infrastructure.

- In addition to the steps and measures outlined above, States should continue 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, and thus contribute to meeting the objectives of this norm.

Elements of implementation

To successfully implement this recommendation, states could consider focusing on supply chain risk, supply chain protections and good non-proliferation practices. The following examples demonstrate how states and organizations have prioritized these elements.

SUPPLY CHAIN RISK

The Japanese government is committed to work in cooperation with private sectors to clarify threats in the supply chain and formulate as well as disseminate frameworks that cut across industrial categories for implementing operational-level measures: “as the supply chain expands globally it is necessary to reflect overseas trends in the development of relevant rules so that cybersecurity measures based on Japan’s security frameworks will be recognized globally”.

Cabinet Office (Japan) (2018) Cybersecurity Strategy

SUPPLY CHAIN PROTECTIONS

The United States National Institute of Standards and Technology (NIST) has conducted extensive work on cyber supply chain risk management and made relevant resources publicly available.

The United States Department of Commerce, National Institute of Standards and Technology, “Best Practices in Cyber Supply Chain Risk Management” (2019)

NON-PROLIFERATION

Forty-two countries have joined the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities.

The Wassenaar Arrangement

Close-up: UNITED STATES

A multi-pronged approach to supply chain security

The Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain* (2019) declared that threats to the information and communications technology and services supply chain by foreign adversaries are a national emergency. The Executive Order prohibited certain transactions that involve information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary whenever the Secretary of Commerce, in consultation with other Federal officials, determines that such a transaction, or a class of transactions:

- Poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;
- Poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or
- Otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.[158]

The February 2021 *Executive Order on America's Supply Chains* commanded several heads of federal agencies to submit status reports and recommendations to the President. These include three directly ICT-related reports:

- (The Secretary of Commerce) a report identifying risks in the semiconductor manufacturing and advanced packaging supply chains and policy recommendations to address these risks
- (The Secretary of Energy) a report identifying risks in the supply chain for high-capacity batteries, including electric-vehicle batteries, and policy recommendations to address these risks
- (The Secretary of Commerce and the Secretary of Homeland Security) a report on supply chains for critical sectors and subsectors of the information and communications technology industrial base, including the industrial base for the development of ICT software, data, and associated services.[159]

To underline the cross-sectorial nature of supply chain security, the White House staff is to coordinate the executive branch actions necessary to implement the order, including recommendations to adjust "the scope for each industrial base assessment, including digital networks, services, assets, and data, goods, services, and materials that are relevant within more than one defined industrial base, and add new assessments, as appropriate, for goods and materials not included in the above industrial base assessments." [160]

[158] The White House (2019). *Securing the Information and Communications Technology and Services Supply Chain*. Executive Order 13873 (15 May 15). Federal Register Vol. 84, No. 96.
[159] The White House (2021). Executive Order on America's Supply Chains. (24 February).
[160] The White House (2021). Executive Order on America's Supply Chains. (24 February).

As the leading federal agency in cybersecurity matters, the Cybersecurity and Infrastructure Agency (CISA) works currently with 20 federal agencies and 40 industry partners in particular through the ICT Supply Chain Risk Management Task Force. Its work consists of:

- Information Sharing Working Group: on proposing paths, such as long-term policy and legal changes, that will give liability protection to the private sector in order to promote information sharing about suspect suppliers.
- Small and Medium-sized Businesses Working Group: engaging the SMB community to understand their needs and tailor Task Force products to make them more applicable to SMBs.
- Product Use Acceleration Working Group: engaging with government agencies; state, local, territorial, and tribal entities; academia; and non-governmental entities on how to apply Task Force products in their businesses, pilot specific products to test their usability, and incorporate feedback to ensure products continue to be useful and provide meaningful information.
- Study Group on Lessons Learned from Recent Software Supply Chain Attacks: diving into how the Task Force can support CIOs, CISOs, and other security personnel in making better risk-informed decisions when procuring or deploying certain ICT products—especially ones with high-level administrative access across an organization.[161]

The Department of Commerce, has continued to create regulations for the processes and procedures to be used to "identify, assess, and address certain transactions, including classes of transactions, between U.S. persons and foreign persons that involve information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and pose an undue or unacceptable risk". In this process, the Department has requested for public inputs and comments. [162]

The United States Department of Commerce, National Institute of Standards and Technology, has published "Best Practices in Cyber Supply Chain Risk Management."[163]

[161] Cybersecurity and Infrastructure Agency (2021). "ICT Supply Chain Risk Management Task Force." https://www.cisa.gov/supply-chain.
[162] Department of Commerce (2021). "Securing the Information and Communications Technology and Services Supply Chain, Interim final rule." Federal Register /Vol. 86, No. 11.
[163] National Institute of Standards and Technology (2020). https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf.

Further examples of implementation

UNITED KINGDOM
Supply Chain Security Guidance
(2020)

British guidance provide organisations with an improved awareness of supply chain security, as well as helping to raise the baseline level of competence in this regard, through the continued adoption of good practice. It centers on twelve principles:
1. Understand what needs to be protected and why
2. Know who your suppliers are and build an understanding of what their security looks like
3. Understand the security risk posed by your supply chain
4. Communicate your view of security needs to your suppliers
5. Set and communicate minimum security requirements for your suppliers
6. Build security considerations into your contracting processes and require that your suppliers do the same
7. Meet your own security responsibilities as a supplier and consumer
8. Raise awareness of security within your supply chain
9. Provide support for security incidents
10. Build assurance activities into your supply chain management
11. Encourage the continuous improvement of security within your supply chain
12. Build trust with suppliers.

The guidance includes also examples of supply chain attacks.[164]

AUSTRALIA
Cyber Supply Chain Risk Management Practitioners Guide
(2019)

Australian guidance emphasizes supply chain risk management as a whole of system life undertaking.

Understand your cyber supply chain. Holistic supply chain management governs a secure supply of products or services to a system, ensuring business continuity and in some cases, national security. It includes the design, manufacture, delivery, support and decommissioning of hardware, software and related services in systems. The cyber security component of supply chain is a significant component of an overall supply chain strategy due to the impact and extent of cyber supply chain exploitation vectors on business.

Know what makes a vendor high risk. A high risk vendor is any vendor that by nature of the product or service they offer, has a significant influence over the security of a system.

Specific Government direction related to supply chain. Government may provide explicit direction where there is legitimate concern over significant non-sovereign ability to control or influence a nationally critical system.

Consistently approach supply chain risk management.

(a) **Know your system.** An organisation must determine criticality of their systems, with regard to sensitivity and business value, especially in a national security context, in order to inform appropriate risk activities.

[164] National Cyber Security Centre (2021). "Supply chain security management." https://www.ncsc.gov.uk/collection/supply-chain-security.

(b) **Understand your supply chain risk.** Make relevant system risk assessments by knowing the systems well, including how they can be exploited and keeping informed of the relevant current threats.
(c) **Manage your supply chain risk.** Objectively manage supply chain alongside other system cyber security risks**.** Avoiding risk may be possible through re-architecture of a system or process in order to minimise the impact of a realised risk. Reducing risk could be accomplished by choosing vendors who have a demonstrated commitment to cyber security from.
(d) **Monitor your supply chain and the controls.** Supply chain and the systems they support will change over time. Regularly monitor and review your SCRM and the controls.[165]

FINLAND
Security of Supply Objectives
(2018)

Security of supply means the ability to uphold society's vital functions in state of emergency. The Government emphasises the importance of safeguarding the basic structures and services essential for the vital functions of society, including both physical facilities and structures as well as electronic functions and services.

National security of supply is increasingly dependent on international cooperation, especially in the case of cross-border risks, such as cyber threats and hybrid influencing. Close international cooperation is also essential in responding to climate change threats, mass migration, communicable diseases, and radiation accidents.

The Ministry of Economic Affairs and Employment is responsible for the overall development of security of supply and the coordination of preparedness measures, while all ministries develop security of supply in their own sectors. The National Emergency Supply Organisation, which is a network of public, private and third-sector operators, develops and maintains Finland's security of supply under the guidance of the National Emergency Supply Agency. [166]

SINGAPORE
CII Supply Chain Programme
(2021)

Singapore is developing a CII Supply Chain Programme - a partnership involving all stakeholders - CSA, CII owners, and their vendors. This programme is to provide recommended processes and sound practices for all stakeholders to manage cybersecurity risks in the supply chain. In addition to improving the stakeholders supply chain security, the program is expected to also help the Government improve its policies around supply chain risks.

[165] Australian Cyber Security Centre (2019). *Cyber Supply Chain Risk Management Practitioners Guide,* p. 1-2.
[166] Ministry of Economic Affairs and Employment (2018). "Valtioneuvoston päätös huoltovarmuuden tavoitteista." https://tem.fi/paatos?decisionId=0900908f805f483d and National Emergency Supply Agency (2021) "Objectives". https://www.huoltovarmuuskeskus.fi/en/security-of-supply/objectives.

	In the longer term, Singapore CII sectors and the companies are also to adopt a zero-trust cybersecurity posture, a shift in mindset necessary to defend supply chain against highly sophisticated threat actors.[167]
JAPAN *Cybersecurity Strategy* (2017)	In the *Cybersecurity Strategy* (2017) Japanese government committed to work in cooperation with private sectors to clarify threats in the supply chain and formulate as well as disseminate frameworks that cut across industrial categories for implementing operational-level measures. In order for business operators. The government emphasized that the contents of the offered guidelines are both realistically feasible and easy to understand. Japan also acknowledged, "as the supply chain expands globally it is necessary to reflect overseas trends in the development of relevant rules so that cybersecurity measures based on Japan's security frameworks will be recognized globally."[168]
UNITED STATES, MEXICO AND CANADA *United States-Mexico-Canada Agreement* (2019)	The 2019 United States-Mexico-Canada Agreement (USMCA) recognizes threats to cybersecurity undermining confidence in digital trade. The USMCA also recognizes risk-based approaches may be being more effective than prescriptive regulation in addressing those threats. Accordingly, the Parties agreed to endeavour to • build the capabilities of their respective national entities responsible for cybersecurity incident response [*cf.* UN GGE 2015 para 13a & 13d] • strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness and best practices [*cf.* UN GGE 2015 para 13d & 13j] • employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.[169] •
FRANCE	In order to strengthen the fight against the proliferation of malicious tools and techniques, France has supported the inclusion of intrusion software on

[167] "Speech by Dr Janil Puthucheary, Senior Minister of State, Ministry of Communications and Information at the MCI Committee of Supply Debate 2021." (2 March 2021). https://www.csa.gov.sg/en/News/Speeches/mci-cos-2021-sms-speech.
[168] Cabinet Office (Japan) (2018). *Cybersecurity Strategy,* p. 18-19.
[169] Office of the United States Trade Representative (2020). *Agreement between the United States of America, the United Mexican States, and Canada,* Chapter 19:15. https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between. Here, the USMCA applies the National Institute of Standards and Technology "Cybersecurity Framework" five concurrent and continuous functions of *Identify, Protect, Detect, Respond, Recover* (https://www.nist.gov/cyberframework and https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf).

Wassenaar Arrangement (2020)

the list of dual-use goods of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. France believes that regulatory efforts must be pursued in this way by including certain cybertools on the list of war materiel, determined in accordance with the gravity of their effects.[170]

Forty-two countries have joined the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. The *Wassenaar Arrangement* has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States will seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists.[171]

In 2013, the Wassenaar Arrangement plenary meeting adopted a set of controls to cover certain law enforcement or intelligence gathering, IP network surveillance systems and intrusion software. This inclusion was contextualized and justified to control technology that "under certain conditions, may be detrimental to international and regional security and stability."[172]

[170] Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General, A/74/120, 24 June 2019. Replies received from governments: France, p. 21.
[171] "The Wassenaar Arrangement." https://www.wassenaar.org/about-us/.
[172] Wassenaar Secretariat (2020). Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, *Public documents, volume IV Background Documents and Plenary-related and Other Statements*, p. 47. https://www.wassenaar.org/app/uploads/2020/12/Public-Docs-Vol-IV-Background-Docs-and-Plenary-related-and-other-Statements-Dec.-2020.pdf

Considerations for practice

- Identify and map national ICT supply chain and relevant stakeholders. Address the integrity of the supply chain in national cybersecurity strategy and policy. Develop a comprehensive supply chain security action plan in cooperation with the private sector.

- Identify baseline level of supply chain security requirements. Include baseline level of supply chain security requirements in national cybersecurity or other relevant legislation. Establish functional public-private partnership with the private sector to consider, prepare and implement measure to ensure supply chain integrity.

- Develop national guidance on enhancing measures to ensure the integrity of the supply chain. Enhance security-by-design thinking and measures by providing guidance to manufacturers. Share, compare and further develop national guidance with relevant nations and corporations.

- Issue deferring Not-Our-Behaviour (NOB)[173] pledge of not mandating backdoor accesses to public communication systems. Invite other stakeholders to join this commitment and participating in its implementation. Develop regional support to and mechanisms for similar statements and commitment on not mandating backdoor accesses to public communication systems.

- Support dedicated transparency centres as ways to ensure the integrity of IT products and process. Facilitate and promote enhancement and refinement of export controls of malicious ICT tools and techniques. Further enhance relevant regional and international non-proliferation frameworks.

[173] Cf. voluntary, non-binding No-First-Use -policy or not allowing the deployment of nuclear weapons to country territory or territorial waters known in the nuclear realm.

Recommendation 10: 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.

GGE 2021 Guidance:

- This norm reminds States of the importance of ensuring that ICT vulnerabilities are addressed quickly in order to reduce the possibility of exploitation by malicious actors. Timely discovery and responsible disclosure and reporting of ICT vulnerabilities can prevent harmful or threatening practices, increase trust and confidence, and reduce related threats to international security and stability.

- Vulnerability disclosure policies and programmes, as well as related international cooperation, aim to provide a reliable and consistent process to routinize such disclosures. A coordinated vulnerability disclosure process can minimize the harm to society posed by vulnerable products and systematize the reporting of ICT vulnerabilities and requests for assistance between countries and emergency response teams. Such processes should be consistent with domestic legislation.

- At the national, regional and international level, States could consider putting in place impartial legal frameworks, policies and programmes to guide decision-making on the handling of ICT vulnerabilities and curb their commercial distribution as a means to protect against any misuse that may pose a risk to international peace and security or human rights and fundamental freedoms. States could also consider putting in place legal protections for researchers and penetration testers.

- In addition, and in consultation with relevant industry and other ICT security actors, States can develop guidance and incentives, consistent with relevant international technical standards, on the responsible reporting and management of vulnerabilities and the respective roles and responsibilities of different stakeholders in reporting processes; the types of technical information to be disclosed or publicly shared, including the sharing of technical information on ICT incidents that are severe; and how to handle sensitive data and ensure the security and confidentiality of information.

- The recommendations on confidence-building and international cooperation, assistance and capacity-building of previous GGEs can be particularly helpful for developing a shared understanding of the mechanisms and processes that States can put in place for responsible vulnerability disclosure. States can consider using existing multilateral, regional and sub-regional bodies and other relevant channels and platforms involving different stakeholders to this end.

Elements of implementation

To successfully implement this recommendation, states could consider focusing on reporting policies, guidance for sharing and implementing of patches. The following examples demonstrate how states and organizations have prioritized these elements.

REPORTING POLICIES

India's National Critical Information Infrastructure Protection Centre (NCIIPC) runs Responsible Vulnerability Disclosure Program for reporting any Vulnerability in Critical Information Infrastructures that may cause unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction of the same.

NCIIPC, "Responsible Vulnerability Disclosure Program" (2017)

GUIDANCE FOR SHARING

The Netherlands has provided an online form and guidelines on how to report a vulnerability. Different procedures have been established for

- security flaws in an ICT system belonging to central government and
- security flaws in another government body (such as a municipality or province) or in an organisation with a vital function (such as an energy or telecoms company).

Government of the Netherlands, "Responsible disclosure" (2021)

IMPLEMENTATION OF PATCHES

Australia has published online guidelines on patching, including different patching approaches, patch management process and procedures.

Australian Signals Directorate, "Systems patching" (2021)

Close-up: JAPAN

Achieving security through transparency

In July 2004, the notice from the Ministry of Economy, Trade and Industry (METI) on "Standards for Handling Software Vulnerability Information and Others" was issued to ensure appropriate handling of vulnerability-related information when a vulnerability is discovered, in order to reduce the damages that could be caused by unauthorized computer access or viruses. Based on these standards, the "Information Security Early Warning Partnership Guideline" defining the recommended actions for relevant parties was established to achieve an appropriate flow of vulnerability-related information.

Specifically, the Information-Technology, Promotion Agency (IPA) serves as the organization to receive reports, while the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) serves as the coordinating organization. These organizations make efforts to handle vulnerability-related information properly with all relevant parties, including discoverers, software/hardware developers and website operators. This process is in alignment with ISO/IEC 29147:2014 "Vulnerability disclosure". It was amended in 2014 and shifted to "Standards for Handling Vulnerability-related Information of Software Products and Others" in 2017.[174]

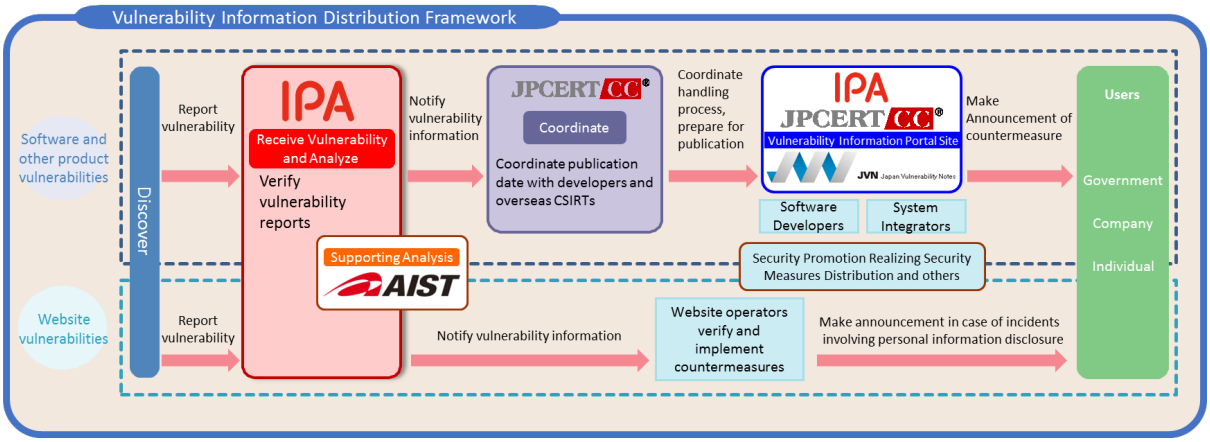
The IPA serves as an organization where people can directly report on security vulnerabilities for analysis. It cooperates with the JPCERT/CC, and related organizations and groups under the framework of the Information Security Early Warning Partnership. The IPA collects information from the internet about vulnerabilities and the ways attackers invent to exploit them. This information is then subject to detailed research and verification, as well as impact evaluation.[175]

When a security vulnerability is discovered, it is reported to the IPA. The IPA will publish information such as what the pertinent products' developers are doing to address the vulnerabilities and any available countermeasures on the Japan Vulnerability Notes (JVN), the portal site operated jointly with the JPCERT Coordination Center, thereby helping protecting users against vulnerabilities.[176]

JPCERT Coordination Center has been assisting vendors' vulnerability handling as a coordinator and publishing advisories on the Japan Vulnerability Notes (JVN) under the Japanese domestic framework "Information Security Early Warning Partnership" since 2004. Internationally, JPCERT/CC also coordinates vulnerability handling in cooperation with CSIRTs in other countries as well as reporters that directly report vulnerabilities to JPCERT/CC.[177] JPCERT/CC is a CNA (CVE Numbering Authority) assigning CVE ID to the reported vulnerabilities, and also a Root CNA recruiting and training CNAs under its umbrella. The *JPCERT/CC Vulnerability Coordination and Disclosure Policy* sets detailed guidelines for reporting.[178] The process is portrayed in the following image.

---

[174] Information-Technology Promotion Agency (2021) "Information Security Early Warning Partnership." https://www.ipa.go.jp/files/000044732.pdf.
[175] Information-Technology Promotion Agency (2021) "Measures for Information Security Vulnerabilities." https://www.ipa.go.jp/security/english/third.html.
[176] Information-Technology Promotion Agency (2021) "Measures for Information Security Vulnerabilities." https://www.ipa.go.jp/security/english/third.html. The Japan Vulnerability Notes portal http://jvn.jp/en/.
[177] JPCERT (2021) "Vulnerability Handling and related guidelines." https://www.jpcert.or.jp/english/vh/guidelines.html.
[178] JPCERT (2019) JPCERT/CC *Vulnerability Coordination and Disclosure Policy*. https://www.jpcert.or.jp/english/vh/vul-coordination-disclosure-policy_2019.pdf.



Japanese vulnerability disclosure process. Source: Information-Technology, Promotion Agency (2021).[179]

It should be noted that although the first and second Japanese *Information Security Strategies* (2006, and 2009, respectively) noted the challenges of vulnerabilities, and their elimination, the 2013 *Cybersecurity Strategy* took up the issue of sharing vulnerability information. This was done in the context of critical infrastructure protection:

For example, "Specifically, promotion of collaboration through information sharing of vulnerability information and attack information, etc. between critical infrastructure providers and cyberspace-related operators, examination of how to introduce evaluation and certification modeled on international standards for procurement and operation of SCADA and other control system equipment and systems, and promotion of measures aimed at establishing institutions for evaluation and certification of control system equipment and systems."[180]

The 2004 ministerial guidance has been sufficient to establish the practice. The 2017 Joint METI and IPA *Cybersecurity Management Guidelines* provides further recommendations for vulnerability analysis and information sharing.[181]

[179] Information-Technology Promotion Agency (2021). "Information Security Early Warning Partnership." https://www.ipa.go.jp/files/000044732.pdf.
[180] Information Security Policy Council (2013). *Cybersecurity Strategy*, p. 35.
[181] Ministry of Economy, Trade and Industry & Information-technology Promotion Agency (2020). *Cybersecurity Management Guidelines* v2.0. https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf.

Further examples of implementation

INDIA
Responsible Vulnerability Disclosure Program (2017)

Indian National Critical Information Infrastructure Protection Centre (NCIIPC), created under the Information Technology Act (2000/2008), runs Responsible Vulnerability Disclosure Program for reporting any Vulnerability in Critical Information Infrastructures that may cause unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction of the same. For that purpose, the NCIIPC hosts the attached Vulnerability Disclosure Form (template) at its website nciipc.gov.in.[182]

NCIIPC Responsible Vulnerability Disclosure

1. Reporter's Details			
a) Full Name			
b) Email			
c)Organisation/Company			
2. Vulnerability Details (✓Check mark)			
a) Vulnerability Name			
b)Vulnerability category	☐ XSS	☐ SQLI	☐ Stack Overflow
	☐ LFI	☐ Click Jacking	☐ User After Free
	☐ XSRF	☐ Information Leakage	☐ Heap Overflow
	☐ Insecure Direct Object Reference		☐ Broken Authentication
	☐ Memory Corruption		☐ Security Misconfiguration
c) Description	(Use Separate Sheet for additional information)		
3. Type of Vulnerability (✓Check mark)	☐ Web Application	☐ Operating System(OS)	
	☐ SCADA	☐ Any Other	
If other please describe in brief			
4. Date when issue found	(dd/mm/yyyy)		
5. Steps to reproduce			
6. Whether POC screenshots/files/documents attached?	☐ Yes	☐ No	
7. Reported to Affected Organisation?	☐ Yes	☐ No	
8. Affected Organisation's name			
9. Affected Organisation's URL			
10. Affected Organisation's email			
11. Vulnerable Product type	☐ Web Application	☐ Client Software	
	☐ Server Software	☐ Firmware	
	☐ Operating System	☐ Hardware	
12. Vulnerable Product name & Version			
13. If reported, Email ID to whom details sent			
14. If reported, date when reported			
15. Patch released?	☐ Yes	☐ No	
16. If patch released, date of patch release	(dd/mm/yyyy)		
17. Anonymity	(Yes/No)		

THE NETHERLANDS
Responsible disclosure (2021)

The Netherlands has provided an online form and guidelines on how to report a vulnerability. Different procedures have been established for

- security flaws in an ICT system belonging to central government and
- security flaws in another government body (such as a municipality or province) or in an organisation with a vital function (such as an energy or telecoms company).[183]

A particular Coordinated Vulnerability Disclosure (CVD) policy has been developed to enable the reporting parties and the organisation to work

[182] Indian National Critical Information Infrastructure Protection Centre (2017). "Responsible Vulnerability Disclosure Program." https://nciipc.gov.in/RVDP.html.
[183] Government of the Netherlands (2021). "Responsible disclosure". https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands/responsible-disclosure.

together in order to reduce the vulnerabilities in IT systems. Implementing this policy should be seen as a supplement to existing measures on information security. The various actors each have their own role and responsibilities. Within the CVD process knowledge is shared with one or more potentially vulnerable organisations in order to arrive at a joint solution for the vulnerability found in collaboration with the reporting party.[184]

AUSTRALIA
Responsible disclosure
(2021)

Australia has published online guidelines on patching, including different patching approaches, patch management process and procedures.

For example, if a patch is released for high assurance ICT equipment, the Australian Cyber Security Centre (ACSC) will conduct an assessment of the patch and may revise the ICT equipment's usage guidance. Where required, the Australian Signals Directorate will conduct an assessment of any cryptographic security vulnerability and may revise usage guidance in the consumer guide or Australian Communications Security Instruction. If a patch for high assurance ICT equipment is approved for deployment, the ACSC will inform organisations of the timeframe in which the patch is to be deployed. [185]

THE UNITED STATES
The Vulnerabilities Equities Policy and Process
(2017)

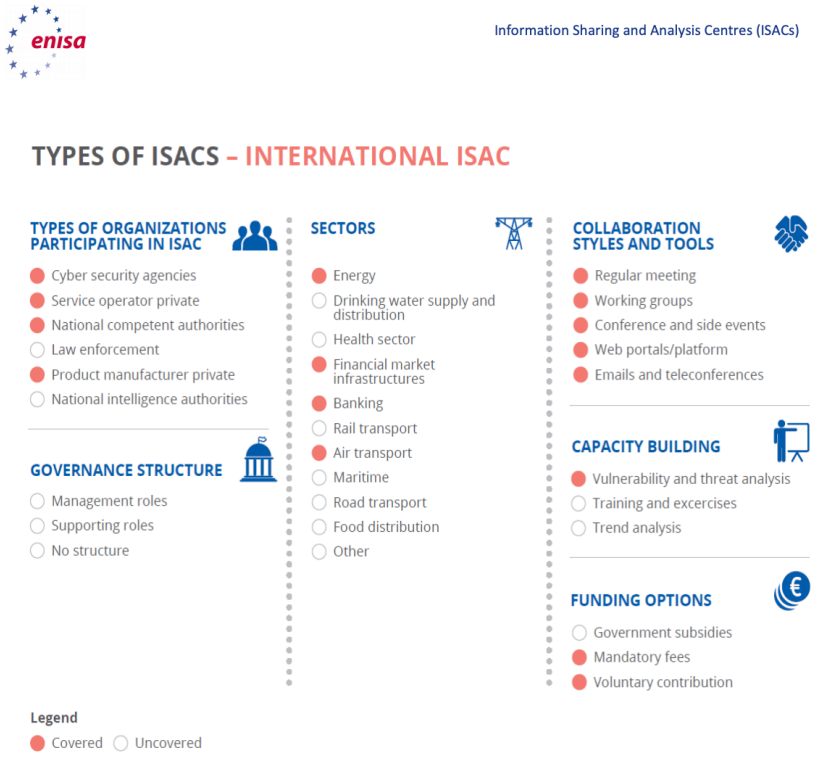
The Vulnerabilities Equities Policy and Process (VEP) for departments and agencies of the United States Government (USG) seeks to balance equities and make determinations regarding disclosure or restriction when the USG obtains knowledge of newly discovered and not publicly known vulnerabilities in information systems and technologies. The primary focus of this policy is to prioritize the public's interest in cybersecurity and to protect core Internet infrastructure, information systems, critical infrastructure systems, and the U.S. economy through the disclosure of vulnerabilities discovered by the USG, absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes.

When an agency determines that a vulnerability reaches the threshold for entry into the process, it will notify the VEP Executive Secretariat as soon as is practicable and provide its recommendation to either disseminate or restrict the vulnerability. The submission will include, at a minimum, information describing the vulnerability, identification of the vulnerable products or systems, and a recommendation on dissemination of the vulnerability information. The VEP Executive Secretariat will notify all VEP POCs within one business day of acknowledging the submission and request that participants respond if they have an equity at stake.[186]

[184] National Cyber Security Centre (2018). *Coordinated Vulnerability Disclosure: The Guideline*.
[185] Australian Signals Directorate (2021). "Systems patching." https://www.cyber.gov.au/acsc/view-all-content/guidance/system-patching.
[186] Vulnerabilities Equities Policy and Process for the United States Government (15 November 2017). https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF; see also the 2012 and 2016 reports at

EUROPEAN UNION
Information Sharing and Analysis Centres (ISACs) Cooperative models
(2020)

The following illustration presents generic international ISAC functions for state-to-state reporting and other information exchanges as outlined by the European Union Agency for Cybersecurity (ENISA).[187]



https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf and https://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf.

[187] For guidance on ISACs, see ENISA (2017). *Information Sharing and Analysis Centres (ISACs) Cooperative models*. https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/at_download/fullReport.

Considerations for practice

- Promote transparency and responsible reporting of vulnerabilities. Adopt legislation and other regulation which encourages and enhances vulnerability disclosures. Support international and sector-specific vulnerability reporting campaigns and mechanisms.

- Establish ways and channels to report vulnerabilities to *e.g.* national cyber security centre or other suitable body. Create mechanisms, such as equities processes, through which standardised handling of disclosed vulnerabilities can happen.

- Create public campaigns on vulnerability risks, mitigation and reporting. Offer key private sector and public actors tailored advice on vulnerability disclosures and management. Support and create 'bug bounty' programs to enhance public-private-civil society joint efforts to disclose vulnerabilities.

- Study best practices and lessons learned from disclosure of vulnerabilities. Promote and support sub-regional or regional vulnerability disclosure mechanisms, including sharing of good practices. Participate in international vulnerability disclosure and management mechanism.

- Create awareness of patching cycles and the importance of software updates. Promote and require timely implementation of available patches.

Recommendation 11: Do no harm to emergency response teams

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.

GGE 2021 Guidance:

- This norm reflects the fact that CERTs/CSIRTs or other authorized response bodies have unique responsibilities and functions in managing and resolving ICT incidents, and thereby play an important role in contributing to the maintenance of international peace and security. They are essential to effectively detecting and mitigating the immediate and long-term negative effects of ICT incidents. Harm to emergency response teams can undermine trust and hinder their ability to carry out their functions and can have wider, often unforeseen consequences across sectors and potentially for international peace and security. The Group underscores the importance of avoiding the politicization of CERTs/CSIRTs and respecting the independent character of their functions.

- In recognition of their critical role in protecting national security, the public and preventing economic loss deriving from ICT-related incidents, many States categorize CERTs/CSIRTs as part of their critical infrastructure.

- In considering how their actions regarding emergency response teams can contribute to international peace and security, States could publicly declare or put in place measures affirming that they will not use authorized emergency response teams to engage in malicious international activity and acknowledge and respect the domains of operation and ethical principles that guide the work of authorized emergency response teams. The Group takes note of emerging initiatives in this regard.

- States could also consider putting in place other measures such as a national ICT-security incident management framework with designated roles and responsibilities, including for CERTs/CSIRTs, to facilitate cooperation and coordination among CERTs/CSIRTs and other relevant security and technical bodies at the national, regional and international levels. Such a framework can include policies, regulatory measures or procedures that clarify the status, authority and mandates of CERTs/CSIRTs and that distinguish the unique functions of CERTs/CSIRTs from other functions of government.

Elements of implementation

To successfully implement this recommendation, states could consider focusing on first response tasks and mandates, supporting emergency cooperation and relevant exercises and drills. The following examples demonstrate how states and organizations have prioritized these elements.

FIRST RESPONSE TASKS AND MANDATES

Ghana (2020) [The Authority shall] ensure that the National Computer Emergency Response Team co-operates with Sectoral Computer Emergency Response Team of other countries in respect of cybersecurity incidents.

Ghana Cybersecurity Act 2020

SUPPORT EMERGENCY COOPERATION

Lao, Burmese and Vietnamese CERTs are members of Asia-Pacific CERT (APCERT) participating in its conferences and exercises. They, together with sixteen other Asia-Pacific nations, also participate in an analytical information exchange mechanism, TSUBAME, a packet traffic monitoring system to observe suspicious scanning activities in the Asia-Pacific region, making their skills, competences and activities rather transparent.

APCERT "TSUBAME Working Group" (2021)

EXERCISES AND DRILLS

Oman CERT's 5th National Cyber Drill, "Malware and the dark Internet: the constant threat" included a number of scenarios for simulating some cybersecurity threats and how they can be handled. Additionally, this drill aimed at enhancing coordination and cooperation between ITA's OCERT and different government and private entities in all sectors.

Oman CERT "5th National Cyber Drill" (2019)

Close-up: THE EUROPEAN UNION AGENCY FOR CYBERSECURITY

Establishing and improving computer security incident response

In establishing, improving and reforming computer security incident response teams and organizations (CSIRT), states can utilize public and private international guidance which clearly outlines the roles and tasks of CSIRTs in line with the purpose of the recommendation 13(k).

In particular, the European Union Agency for Cybersecurity (ENISA) guidance, over 60 reports in supporting CSIRT establishment, training and operations, is worth examining. That ENISA guidance is tailored for the European Union Member States needs should not discourage but encourage other governments to follow it as the guidance is neutral to any particular form of political or administrative culture. The guidance is useful to be analysed also when reforming the normative and administrative (governance) frameworks within which CSIRTs operate. Moreover, as the EU Member States are keen supporters of rule based public international order in general and subscribe to the 2015 UN GGE framework of responsible state behaviour in cyberspace, the CSIRT guidance can be expected to follow the spirit of the recommendation 13(k), too.

The 2020 ENISA report "How to set up CSIRT and SOC", describes CSIRT tasks and role followingly:
"CSIRT has become a generic name for a team that provides a set of services: information and cybersecurity incident handling (core service), security monitoring, vulnerability management, situational awareness and cybersecurity knowledge management.

In simpler terms, CSIRT is a team that is assigned to handle computer security (thus, often, cybersecurity) incidents. Often this includes additional responsibilities, from detection to analysis, and even hands-on fixing, as well as different situational awareness, knowledge transfer and vulnerability management activities. Over the years, the role of a CSIRT has evolved from providing incident monitoring and handling services to coordinating and communicating with different stakeholders, countries and specific sectors.

Currently, FIRST.org hosts and continuously improves a CSIRT Services Framework, which is a high-level document that describes the activities carried out by CSIRTs. These activities are organised into five main service areas, which are further split into services, functions and subfunctions. A CSIRT can choose which of the services and functions are relevant to their mandate and organise them into their own services structure." [188]

The report emphasises the importance of CSIRT mandate, the purpose – the initial idea, reasons and justification why a CSIRT is needed. In this process inclusion and transparency not only secure comprehensive professionalism and creates mutual trust but also de-mystifies national cyber security activities:
"1. Identifying all major stakeholders and understanding their needs and expectations of a CSIRT. Depending on the stakeholder, their needs can include identification of incidents, security awareness, resolution of incidents and compliance with certain standards.

[188] ENISA (2020) "How to set up CSIRT and SOC", p. 6. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc.

2. Identifying constituencies. This could be a small group of companies for a sectorial CSIRT, the residents of a city or even a whole country. Evaluating and meeting the needs and expectations of a specific constituency are extremely important for the success of a CSIRT." [189]

Parliamentary involvement, and the inherent political debate, is as necessary:
"For national governments or sectoral regulators, the development of a mandate usually begins with drafting of a law, bill, cybersecurity strategy or cybersecurity plan." [190]
Accordingly, oversight mechanisms, "Who will provide direction, monitoring and oversight of the CSIRT?", [191] within incident response governance system support adherence of the recommendations and remove potential doubts elsewhere.

Finally, inclusively developed service and training plans and processes, which are to be nationally and internationally tested and exercised, safeguard the appropriate direction and operations of national or sectoral CSIRTs. [192]

[189] ENISA (2020). "How to set up CSIRT and SOC", p. 14, 19-20.
[190] ENISA (2020). "How to set up CSIRT and SOC", p. 15.
[191] ENISA (2020). "How to set up CSIRT and SOC", p. 16.
[192] ENISA (2020). "How to set up CSIRT and SOC", p. 20-25.

Further examples of implementation

LAOS, BURMA AND VIETNAM *APCERT cooperation* (2021)	Lao, Burmese and Vietnamese CERTs operate under ministries Post and Telecommunication, Communication and Technology, and Information and Communications, respectively and are members of Asia-Pacific CERT (APCERT) participating in its conferences and exercises. They, together with sixteen other Asia-Pacific nations, also participate in an analytical information exchange mechanism, TSUBAME, a packet traffic monitoring system to observe suspicious scanning activities in the Asia-Pacific region, making their skills, competences and activities rather transparent.[193]
AZERBAIJAN *Computer Emergency Response Center:* *(2021)*	Azeri Computer Emergency Response Center operates under Special Communication and Information Security State Service of the Republic of Azerbaijan. The Center is tasked with mutual activity and cooperation with relevant agencies, foreign "CERT" teams on issues of computer crimes and legal provision of information security, information and work practice exchange.[194]
BRUNEI *Reply to UN Secretary-General* (2017)	The Brunei national computer emergency response team was established in May 2004 and became the nation's one-stop referral agency in dealing with computer-and Internet-related security incidents. Through a global affiliation with other computer emergency response teams, the national team acquires valuable information on security threats to information and communications technology (ICT) and shares findings on security risks detected within the nation's ICT infrastructure.[195]
SERBIA *Reply to UN Secretary-General* (2019)	National CERT monitors the status of incidents on national level, provides early warnings, alerts and announcements, and reacts on incidents by providing the information on affected entities and persons, makes risk assessments and raises awareness on information security issues. It is regulated that the National CERT will cooperate with the similar organizations in other countries. The Law also regulates the crypto security and the protection against the compromising electromagnetic emanation.[196]
GHANA *Cybersecurity Act* (2020)	Ghana *Cybersecurity Act* stipulates that [The Authority shall] ensure that the National Computer Emergency Response Team co-operates with Sectoral Computer Emergency Response Team of other countries in respect of cybersecurity incidents.[197]

[193] APCERT (2021). "TSUBAME Working Group." https://www.apcert.org/about/structure/tsubame-wg/index.html#Members.
[194] https://cert.gov.az/en/pages/2
[195] Developments in the field of information and telecommunications in the context of international security, A/72/315 11 August 2017submission by Brunei Darussalam, page 7.
[196] Developments in the field of information and telecommunications in the context of international security
Report of the Secretary-General, A/74/120, 24 June 2019. Replies received from governments: Serbia, p. 2.
[197] *Ghana Cybersecurity Act 2020, (43 (1) b).*

THAILAND *ThaiCERT: About Us* (2021)	ThaiCERT collaborates with Thai government sector, organizations, universities, ISPs and other relevant entities to handle computer security incidents in Thailand. Additionally, as a full and active member of Forum of Incident Response and Security Teams (FIRST) and Asia Pacific Computer Emergency Response Team (APCERT), ThaiCERT coordinates with both globally and regionally trusted CSIRTs in responding to computer security incidents.[198]
EUROPEAN UNION *CERT Exercises Handbook* (2015)	The European Union Agency for Cybersecurity (ENISA) exercise handbook, guiding the European computer emergency response team exercises focuses, on the scenarios of a phishing attack, botnet, internal worm outbreak and large-scale DDoS attack exercising and developing incident management and resolution skills. The scenarios or suggested handlings do not refer to any military operations or skills or offensive activities.[199] ENISA has analysed cooperation cooperation between computer security incident response teams (CSIRT), in particular national and governmental CSIRTs, and law enforcement agencies and their interactions with the judiciary (prosecutors and judges). The report proposes a methodology to analyse the legal and organisational framework, the roles and duties of CSIRTs, LEAs and the judiciary, and their required competences, as well as synergies and potential interferences in their activities related to their responses to cyber incidents and fight against cybercrime, respectively.[200]
THE UNITED STATES *Operations doctrine* (1992-)	When developing cyber military capabilities, the United States has anchored them in international law, International Humanitarian Law, in particular, and has been transparent on the purpose and direction of military cyberspace operations through publishing ministerial (department) and joint doctrines and field manuals and other publicly available steering documents.[201]
OMAN *National Cyber Drill* (2019)	The 5th National Cyber Drill, "Malware and the dark Internet: the constant threat", Oman CERT organized in 2019 exposed (70) government and critical infrastructure sector (including finance, telecommunication, energy, transportation, aviation and health) participants to various scenarios based on case studies, latest security incidents and real-life situations.

[198] ThaiCERT (2021). "About us." https://www.thaicert.or.th/about-en.html.
[199] ENISA (2015). *CERT Exercises Handbook*. https://www.cert.pl/wp-content/uploads/2015/12/Large-Scale-Incident-Handling-handbook.pdf; ENISA Good Practice Guide on National Exercises Enhancing the Resilience of Public Communications Networks.
[200] ENISA (2021). *Report on CSIRT – LE Cooperation. A study of the roles and synergies among selected EU Member States/EFTA countries.* https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation. See also, ENISA (2020) *Roadmap on the cooperation between CSIRTS and LE*. https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation.
[201] See for example, Department of Defense (2001 and 2006). Directive S-3600.1, "Information Operations (U)"; (2011) *Department of Defense Strategy for Operating in Cyberspace*; and (2018) *Summary. Department of defense Cyber Strategy*; Joint Chiefs of Staff (1992). *Joint Doctrine for Command and Control Warfare* (JP 3-13.1); (1998) *Joint Doctrine for Information Operations* (JP 3-13); and (2013 and 2018) Cyberspace Operations (JP 3-12); U.S. Department of Army (2014). *Cyber Electromagnetic Activities* (FM 3-38).

The event focused on building human national capabilities of government entities and national critical infrastructure to handle all kinds of cybersecurity incidents and to enhance their readiness and preparedness to respond to these incidents. The drill included implementing a number of scenarios for simulating some cybersecurity threats and how they can be handled through Cybersecurity Readiness Teams "CERTS" as well as measuring the response rate between participating teams to ensure continuation of joint efforts to address cyber threats.

Additionally, this drill aimed at enhancing coordination and cooperation between ITA's OCERT and different government and private entities in all sectors.[202]

OAS
Strengthening the Cyber Security Capacity of the Americas
(2016)

The Organization of American States (OAS) set in its cybersecurity program among the main objectives the establishment of national computer security incident response teams (CSIRTs) in each OAS member country. Moreover, a creation of a hemispheric watch and warning network made up of these CSIRTs would provide guidance and support to cyber security technicians from around the Americas.

International exercises with hundreds of public and private participants as well the established CSIRTamericas.org help to maintain emergency response team focus, competences and activities focussed the originally intended purposes.[203]

[202] Oman CERT (2019). "5th National Cyber Drill "التمرين الوطني الخامس لمن السيبراني. https://www.cert.gov.om/library/publications/FinalNationalDrill_Vendors_v2.pdf.

[203] Organization of American States (2021). "Cyber Security." https://www.sites.oas.org/cyber/en/pages/default.aspx; and (2016) "Strengthening the Cyber Security Capacity of the Americas The OAS Cyber Security Program." http://www.oas.org/es/sms/cicte/IGF-OAS.pdf.

Considerations for practice

- Acknowledge and respect the culture of trust and independence of thought and action that underpins the establishment and functioning of emergency response community. Avoid over-regulation and excess formal requirements of computer emergency response activities. Explicitly encourage technical-level cooperation with all other countries.

- Focus emergency response team mandates to incident mitigation, management and recovery tasks. Maintain national/state emergency response team autonomy from intelligence and security services and the military authorities. If developing cyber military operational capabilities, publish a cyber operations doctrine and rules of engagements.

- Issue deferring Not-Our-Behaviour (NOB)[204] commitment not to harm or exploit emergency response teams. Invite other stakeholders to join this commitment and participating in its implementation. Develop regional support to and mechanisms for similar statements and commitment not to harm or exploit emergency response teams.

- Promote cooperation between different national first response teams. Promote cooperation between first response teams through national, sectorial, regional and international cooperation frameworks.

- Train and conduct exercises for civilian and societal incident management skill set and with such scenarios. Participate in international exercises to increase transparency and foster mutual trust. Design international and cross-sectorial exercises where civilian, peaceful, cooperative and problem-solving attitudes are emphasized over retaliatory or coercive.

[204] Cf. voluntary, non-binding No-First-Use -policy or not allowing the deployment of nuclear weapons to country territory or territorial waters known in the nuclear realm.

Procedural Guidance

Implementation of the recommendations, or any national endeavour, does not happen under its own weight. It requires a holistic approach involving politically determined, governmentally guided and organised cooperative action. As the Qatari *National Cyber Security Strategy* (May 2014, p. 17) outlines:

> Successful implementation of the NCSS requires continuous commitment, governance, and action by various stakeholders who are collectively responsible for the national approach to cyber security. These stakeholders are connected by a shared set of guiding principles (…)

Before starting to implement the recommendations, each country needs to determine both the role of ICTs in national activities and its goals – this will help to prioritize the recommendations, set realistic goals and assess the impact of implementation. An important element in this process is understanding the outcomes that the GGE's 2015 recommendations are intended to achieve. The overall aim is to prevent malicious and hostile usage of ICTs with a clear focus on international peace and security. To fully understand the importance of each recommendation, each country must consider the context, scope and possible modalities of implementation, which include domestic and international ambitions, available resources and international commitments and obligations.

By taking norms-relevant steps, developing and employing competences and capacity in a cooperative and peaceful manner, countries confirm they are taking as serious their commitment to a free, open, stable and secure cyberspace.

The following framework, involving the aspects of orienting, organising and optimising, offers detailed advice as to how that commitment be initiated, sustained and renewed. The three aspects of the framework can be sequential, parallel and oscillating depending on the given situation. Implementing the recommendations is rarely a linear process![205]

Orient: countries/individuals should become acquainted with the situation, and grasp the essential aspects of both the recommendations and the ICT environment

- Determine purposes and objectives of the recommendation
  - what is the issue, problem and direction?
- Analyse national state of cyber affairs
  At what stage of development are we?
  - do we have such a problem? How does this problem materialize? How severe is this problem?

[205] For additional guidance and information on national strategy development and implementation, see Bibliography (below).

- do/don't we already have the measures and mechanisms which deal with the issue?[206]
- do we need to take action?
- what outcomes do we seek?
- what shall we prioritize?

How do we achieve these outcomes?
- do/don't we already have the measures and mechanisms, which deal with the issue?[207]
- do we have the resources to do this?

- Determine prioritization of objectives as well as recommendations to be implemented
- Determine key measures to be taken within each objective and norm

Organise the work to be done:

- Establish a steering group with cross-governmental and multi-stakeholder participation
- Analyse how cybersecurity governance system or processes can be used in implementing the recommendations with readiness to reorganise some structures, processes or work
- Establish working groups according to determined objectives and recommendations
- Determine key stakeholders who can add value to implementing the recommendations
- Determine value-adding roles and responsibilities for each stakeholder

Optimise: write implementation in! Concrete and understandable goals, feasible measures and methods and explicitly assigned roles, responsibilities and resources become quality signs of strategic and administrative skilfulness

- Use the action plan to explicitly communicate the governmental objectives and the assigned tasks and responsibilities[208]
- Conduct frequent cross-sectorial and multi-stakeholder dialogue and engagement
- Determine the financing principles for the action to be taken[209]
- Determine measurable metrics[210]
- Adopt checklists[211]
- Conduct exercises to train, test and evaluate processes and progresses
- Review and renew policies, strategies, plans and programs
- Engage in and contribute to bilateral, regional and global cybersecurity processes and programs.

[206] In this context, the capacity elements of legal, policy, organisation, procedures, financing, technology, human resources, and skills and competences as an analytical framework or even a checklist can be used.
[207] In this context, the capacity elements of legal, policy, organisation, procedures, financing, technology, human resources, and skills and competences as an analytical framework or even a checklist can be used.
[208] See, for example, *The 2014 Mauritius National Cyber Security Strategy 2014-2019*, p. 18.
[209] See, for example, *Vietnam's Cybersecurity Strategy by 2020* (2016), Section V.
[210] See, for example, Philippines *National Cybersecurity Plan 2022* (2020), p. 43.
[211] Singapore will develop a checklist of the steps that countries will need to take to implement a set of norms on cyber security and responsible state behaviour in cyberspace. The 2019 chart will be refined and made applicable for more UN member countries, taking into account their national priorities and capabilities. The ASEAN group will also share its experience and knowledge with the UN so that other countries, especially developing nations, can identify the steps they need to take to implement the norms, such as establishing legal frameworks and developing information sharing networks. (Minister for Communications and Information S. Iswaran (9 Oct 2020), https://www.straitstimes.com/singapore/politics/singapore-un-to-cooperate-on-checklist-for-countries-to-implement-cybersecurity)

Bibliography

All national information or cybersecurity strategies referred to in the footnotes can be accessed through the GFCE's Cybil Portal.

United Nations

United Nations General Assembly

UN General Assembly (1999) Resolution, Developments in the field of information and telecommunications in the context of international security. UN Doc. A/RES/53/70 (4 January).
UN General Assembly (2003) Resolution, Developments in the field of information and telecommunications in the context of international security. A/RES/58/32 (18 December).
UN General Assembly (2006) Resolution, Developments in the field of information and telecommunications in the context of international security. A/60/45 (6 January)
United Nations General Assembly (2018) Resolution, Developments in the field of information and telecommunications in the context of international security. A/73/27 (5 December).
United Nations General Assembly (2018) Resolution, Advancing responsible State behaviour in cyberspace in the context of international security. A/RES/73/266 (22 December).
United Nations General Assembly (2010) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/65/201 (30 July).
United Nations General Assembly (2013) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/68/98 (24 June).
United Nations General Assembly (2015) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174 (22 July).
United Nations General Assembly (2017) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/72/327 (August 14).

United Nations Open-ended Working Group (2019-2021) (https://www.un.org/disarmament/open-ended-working-group/)

Country comments, submissions and working papers
Joint proposals
Informal multi-stakeholder consultations (25 February 2021)
Contributions, comments and informal papers by Inter-governmental Organizations and Non-Governmental Organizations
Documents of the informal meetings of the OEWG
Draft substantive report (Zero draft) (A/AC.290/2021/L.2)
Draft substantive report (First draft)
Final Substantive Report (Conference room paper) (A/AC.290/2021/CRP.2)

United Nations Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (2019-2020)

Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security. Advance copy. (28 May 2021).

United Nations International Telecommunication Union
Resolution, Strengthening the role of ITUin building confidence and security in the use of information and communication technologies. Res. 130 (REV. Dubai, 2018).

National statements and guidance on the implementation of the UN GGE recommendations

"Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015." Foreign and Commonwealth Office. September 2019.

"Summary of public submissions on developing best practice guidance on implementation of the 11 norms of responsible state behaviour in cyberspace articulated in the 2015 GGE Report (A/70/174), as endorsed by the UN General Assembly (A/RES/70/237)". Australian Department of Foreign Affairs and Trade. June 2020.

"Canada's implementation of the 2015 GGE norms." Global Affairs Canada. November 2020.

Open Ended Working Group Developments in the field of information and telecommunications in the context of international security (2020) Joint Proposal: Argentina, Australia, Canada, Chile, Denmark, Estonia, France, Indonesia, Kenya, Mexico, the Netherlands, New Zealand, Pacific Island Forum member states, Poland, and South Africa on "National Survey of Implementation of United Nations General Assembly Resolution 70/237". https://www.dfat.gov.au/sites/default/files/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf

Further work on voluntary, non-binding recommendations

Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary. New York, UN ODA, 2017.

Global Commission on the Stability of Cyberspace (2018) "Norms package Singapore.".
Global Commission on the Stability of Cyberspace (2019) "Advancing Cyberstability. Final report."

"Possible ways to implement the UN GGE norms and capacities required." 4th ASEAN Ministerial Conference on Cybersecurity. Singapore, 2 October 2019.

Tech Accord (2020) "Cybersecurity Tech Accord submission to Australian consultation on: Responsible state behavior in cyberspace." (2 March).

Additional guidance and information on national strategy development and implementation

United Nations International Telecommunication Union (2018) *Guide to Developing a National Cybersecurity Strategy*.

United Nations International Telecommunication Union (2016) “National Cyber Security Strategy (NCS) Toolkit.” https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf.

United Nations Institute for Disarmament Research (2019) “UNIDIR Cyber Policy Portal.” https://unidir.org/cpp/en/.

The World Bank (2020) “Global Cyber Security Capacity Program Phase I and II: Strengthening national Cyber Security Environment of Selected Developing Countries.” https://www.worldbank.org/en/news/feature/2020/06/01/kwpfgscp.

European Union Agency for Cybersecurity (2021) “National Cybersecurity Strategies.” https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

World Economic Forum (2021) “Centre for Cybersecurity”. https://www.weforum.org/platforms/the-centre-for-cybersecurity.

Global Cyber Security Capacity Centre, Oxford University (2021) “The Cybersecurity Capacity Maturity Model for Nations.” https://gcscc.ox.ac.uk/cmm-2021-edition.

United Kingdom’s Multi-stakeholder Advisory Group on Cyber Issues (2019) “Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015.”