

Contribution of the Geneva Dialogue on Responsible Behaviour in Cyberspace to the UN Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021–2025

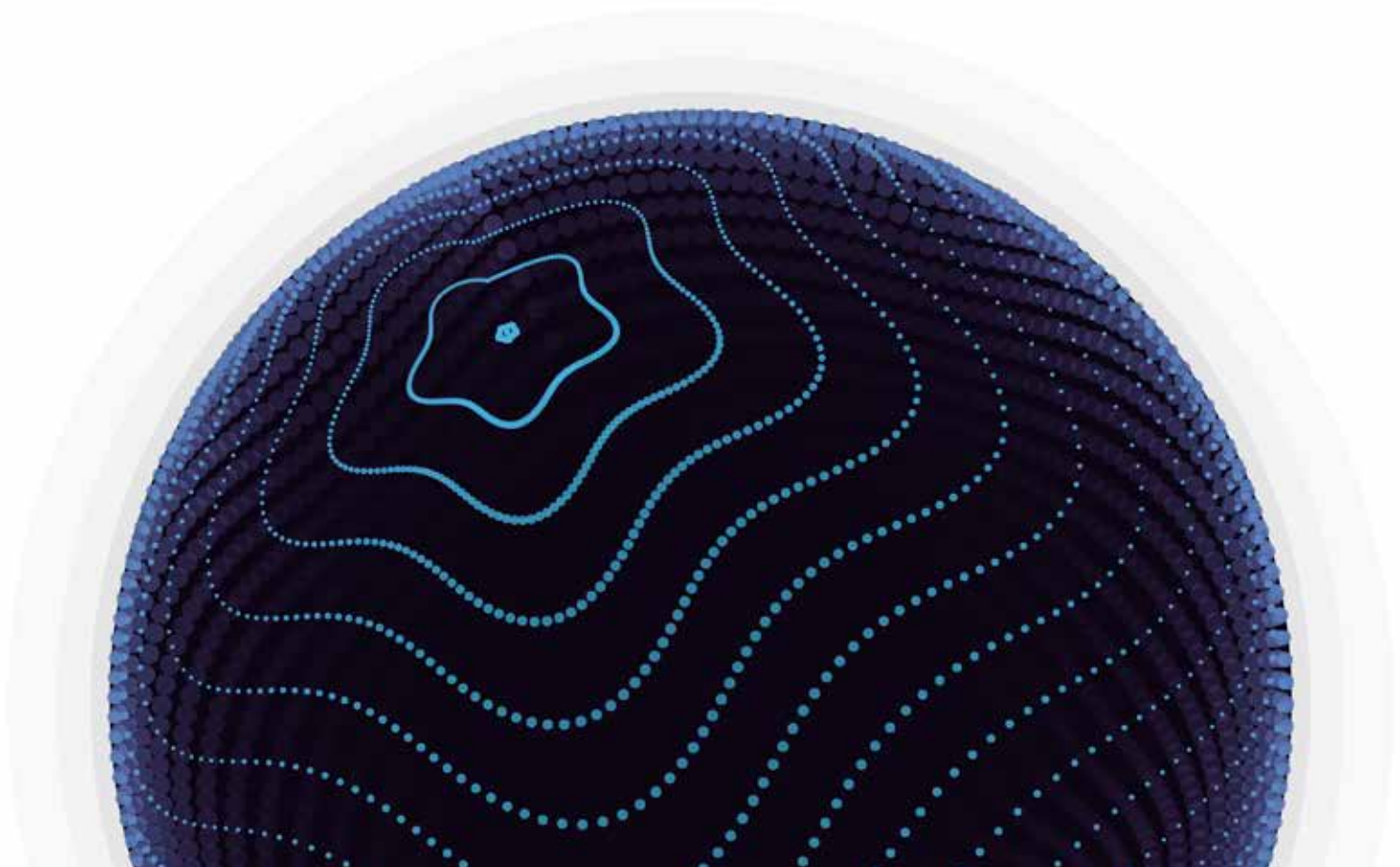
GENEVA MANUAL

On Responsible Behaviour in Cyberspace

Implementation of Agreed Norms and Confidence-Building Measures by Relevant Non-State Stakeholders to Protect Critical Infrastructure

Chapter 2

March 2025





CONTENTS

Executive summary	4
What is the Geneva Manual?	6
How do norms guide stakeholders in protecting critical infrastructure?	9
Key messages: How do non-state stakeholders understand and interpret the implementation of the agreed CIP related cyber norms and CBMs?	13
Key roles and responsibilities: How can non-state stakeholders protect CI?	22
Role: CI operators/owners	22
Role: Product vendors and service providers	25
Role: Cybersecurity research and incident response experts	29
Role: Open source software (OSS) actors	32
Role: Civil society engaged in advocacy, research, training, and communications	33
Conclusion	36
Annex	38
Comparative analysis of how states approach CIP	38
UN GGE Norms and CBMs	60
Contributors	62

EXECUTIVE SUMMARY

The Geneva Dialogue on Responsible Behaviour in Cyberspace, established by the Swiss Federal Department of Foreign Affairs, and led by DiploFoundation with the support of the Republic and State of Geneva, Center for Digital Trust (C4DT) at EPFL, Swisscom, and UBS, addresses the roles and responsibilities of relevant non-state stakeholders in ensuring the security and stability of cyberspace.

Emphasising the principle of shared responsibility, the Geneva Dialogue focuses on operationalising the UN cyber norms by the private sector, academia, civil society, and the technical community to contribute to global cyber security and peace. The results are published in the **Geneva Manual**, the key outcome of the Geneva Dialogue, reflecting contributions from over 50 entities and experts around the world. The Geneva Manual documents stakeholders' understanding of the UN cyber norms, their agreements and disagreements on particular aspects of their implementation, and provides guidance for international collaboration, while outlining the related good practices. Thus the **Geneva Dialogue makes an important contribution to the international discussions, including in the UN Open-ended Working Group (OEWG), by advancing the implementation of the agreed norms and promoting responsible behaviour in cyberspace.**

The second chapter of the Geneva Manual complements the inaugural edition by continuing the discussion on the implementation of the agreed norms and expanding the scope to the three UN GGE norms related to critical infrastructure protection (UN GGE norms F, G, and H) and operationalisation of confidence-building measures (CBMs). These efforts also rely on earlier [results of the Geneva Dialogue](#) to collect good practices by industry and private sector in reducing vulnerabilities in digital products and securing their design and development.

The Geneva Manual highlights the diverse perspectives of non-state stakeholders, emphasising the **importance of multistakeholder participation in the implementation of norms**. It not only provides a comprehensive framework for multistakeholder collaboration but also offers policymakers and the cyber diplomacy community feedback on the interpretation and understanding of the agreed norms from a non-state stakeholder perspective, and thus hopefully provoking further discussions and informing policymakers' efforts to protect CI, including within the UN OEWG. The identified diverse views could also, hopefully, contribute to the **norms implementation checklist proposed by the UN OEWG Chair**.¹ These message include:

- **Cross-jurisdictional interdependencies:** Non-state stakeholders can support states by identifying and mapping interdependencies between CI in the cyber domains, including related to the technical infrastructure crucial for the general availability and integrity of the Internet. The goal is to analyse cause-and-effect relationships and possible cascading failures between such interdependencies, and therefore to pinpoint security challenges and recommend steps to ensure adequate protection of these interconnected assets, systems, and networks against current threats.
- **Transparency vs. secrecy in CI identification:** While states maintain secrecy in CI designation for national security reasons, greater transparency about how states define CI and approach the CI protection in line with the agreed framework of responsible behaviour in cyberspace is needed for non-state stakeholders to meaningfully contribute. By adopting a layered approach to information sharing –where general information about CI definitions and protection strategies is shared while sensitive details remain confidential – policymakers can strike a balance between maintaining security and ensuring broader, collaborative engagement of relevant stakeholders.

¹Chair's Discussion Paper on a Checklist of Practical Actions for the implementation of voluntary, non-binding norms of responsible State behaviour in the use of ICTs [Initial Draft], ANNEX B, 20 FEBRUARY 2024, available at https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/Letter_from_OEWG_Chair_20_February_2024.pdf

- **Commonly accepted cybersecurity requirements for CIP:** The lack of commonly accepted (across jurisdictions) cybersecurity requirements across jurisdictions may create challenges and delays for effective CI protection. Non-state stakeholders, particularly CI owners/operators, product vendors and service providers, the technical community, including cybersecurity experts and others, can collaborate with policymakers to define risk-based baseline requirements for CI security and harmonise regulatory frameworks for incident handling and software supply chain security.
- **Industrial Control Systems (ICS) vulnerabilities:** The unique challenges of updating and securing ICS used in CI sectors require targeted solutions. Relevant stakeholders, including, specifically, product vendors and service providers, should promote security-by-design, while CI operators/owners and the cybersecurity community need to foster partnerships for vulnerability research. Academia and civil society engaged in advocacy and policy can assist in exploring solutions to address barriers to timely updates that balance operational safety and cybersecurity needs.
- **Cross-border cooperation for the technical community:** Geopolitical tensions impact cybersecurity and complicate cross-border collaboration among cybersecurity researchers, incident response experts, and within the decentralised open-source community. Promoting frameworks that protect responsible disclosure and support international cooperation is vital for building trust and resilience in CI systems.
- **Exploring the interpretation of the UN GGE norm F to address non-physical, as well as non-intentional or secondary/collateral, damage from cyber activities targeting or impacting CI:** The norm F explicitly focuses on intentional physical damage but may overlook non-physical effects, such as service disruptions and data breaches, which can have severe societal and economic impacts. Non-state stakeholders can assist policymakers in developing guidelines to classify and address these intangible and non-intentional harms as well as developing approaches to quantify the impact, contributing to the evidence-based risk assessment and development of effective CIP measures.
- **Clarifying the application of the agreed framework amid conflicts:** The evolving role of various private actors in modern conflicts highlights legal ambiguities that can leave CI operators/owners, product vendors and service providers, as well as cybersecurity experts uncertain about their responsibilities and exposed to evolving risks that are harder to anticipate or defend against. These stakeholders need policymakers' guidance on the application of international law, voluntary cyber norms and CBMs to avoid escalation and ensure effective CI protection during conflicts.

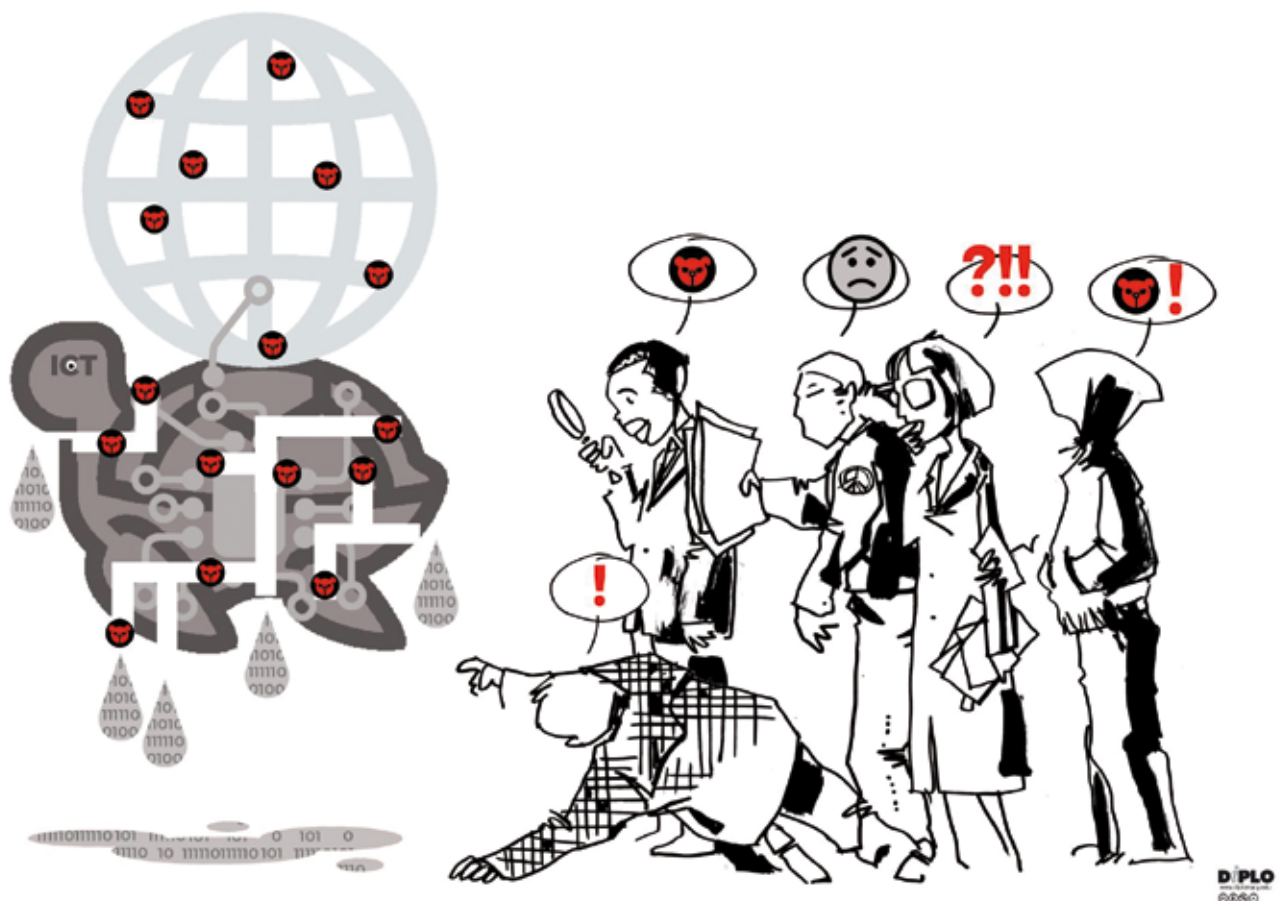
The Geneva Manual further identifies practical, targeted recommendations for various stakeholders, promoting the implementation of the UN GGE norms and responsible behaviour in cyberspace. The key message is the critical need for these diverse actors to move beyond observation and take active roles as key contributors to the implementation of the agreed cyber norms and CBMs. Collaboration is not merely an option – it is a necessity to address cyber risks for CI.

The Geneva Dialogue will continue discussions on these open questions, and clarify the respective roles and responsibilities of stakeholders in the implementation of the UN framework on responsible behaviour and cyber norms, in particular. Interested stakeholders are invited to contribute to future work of the Geneva Dialogue.

WHAT IS THE GENEVA MANUAL?

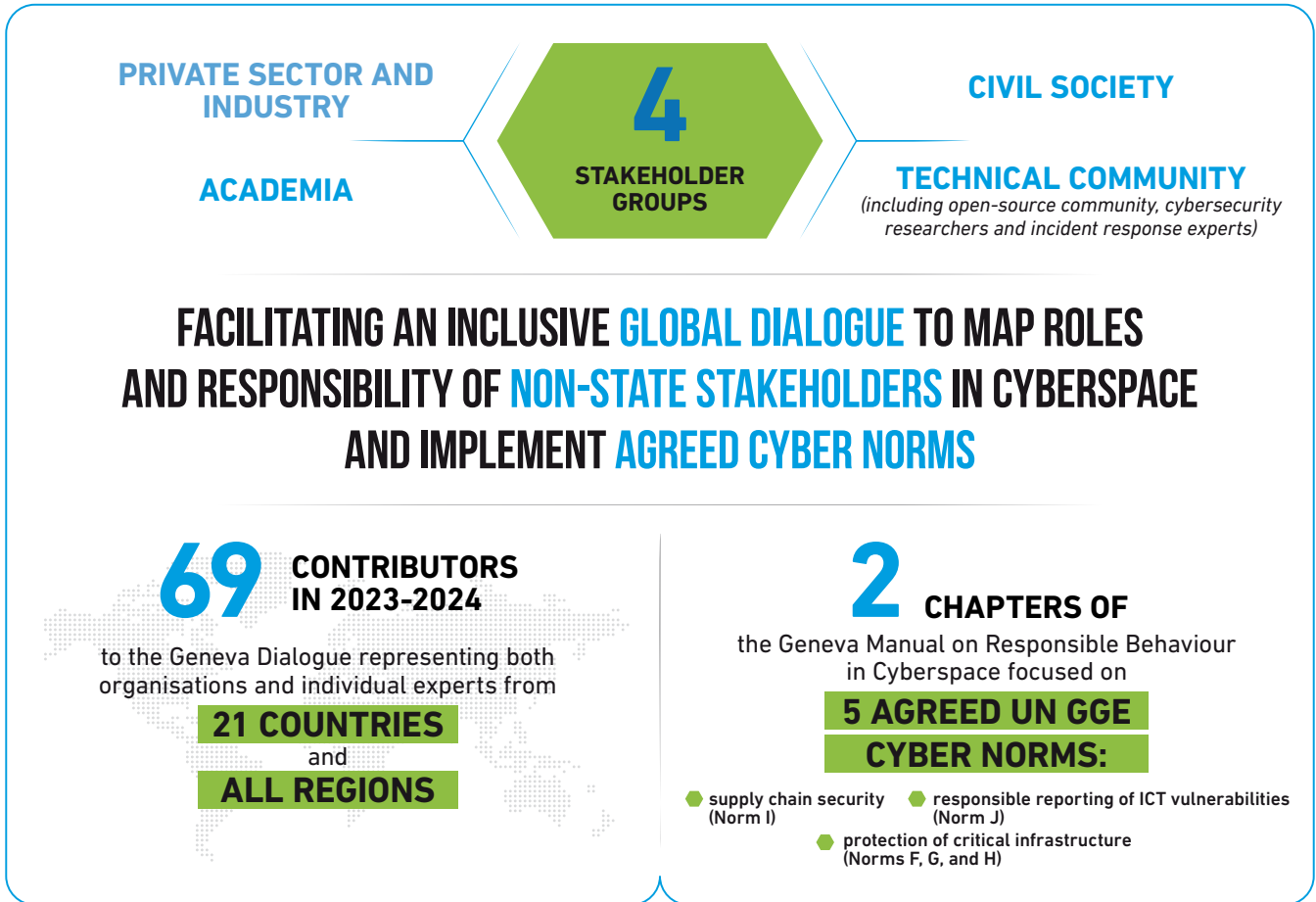
Six *United Nations Groups of Governmental Experts (GGE) on information and communications technology (ICTs)* have been convened since 2004, resulting in a UN normative framework to promote responsible state behaviour in cyberspace (further referred to as 'cyber-stability framework') which includes four pillars: international law, 11 voluntary non-binding norms, confidence-building measures (CBMs), particularly to improve transparency, predictability and stability in the digital space, and capacity building. In 2021, this framework was endorsed and reaffirmed by all the UN member states through adopting the final report of the *UN Open-ended working group (OEWG)*.

However, the ICT infrastructure that makes the digital space such a unique and valuable place is neither owned or operated by states, nor do states have the sole ability to govern it, due to its transnational nature. In fact, most of the ICT infrastructure is owned and operated by thousands of private companies, which also produce the devices, from traditional computers to medical devices, connecting to, and utilising the internet. In addition, technical community sets the standards and has the hands-on knowledge and expertise on running and securing the ICT environment, while civil society, with its broad understanding of social and economic context, wide networks, and ability to reach out to end-users, plays and can play an important role to enhance citizens' awareness and advocate for their safety and rights.



These stakeholders are often only spectators to the normative processes by states, yet, in the end, they play an important role for the implementation of this normative framework.

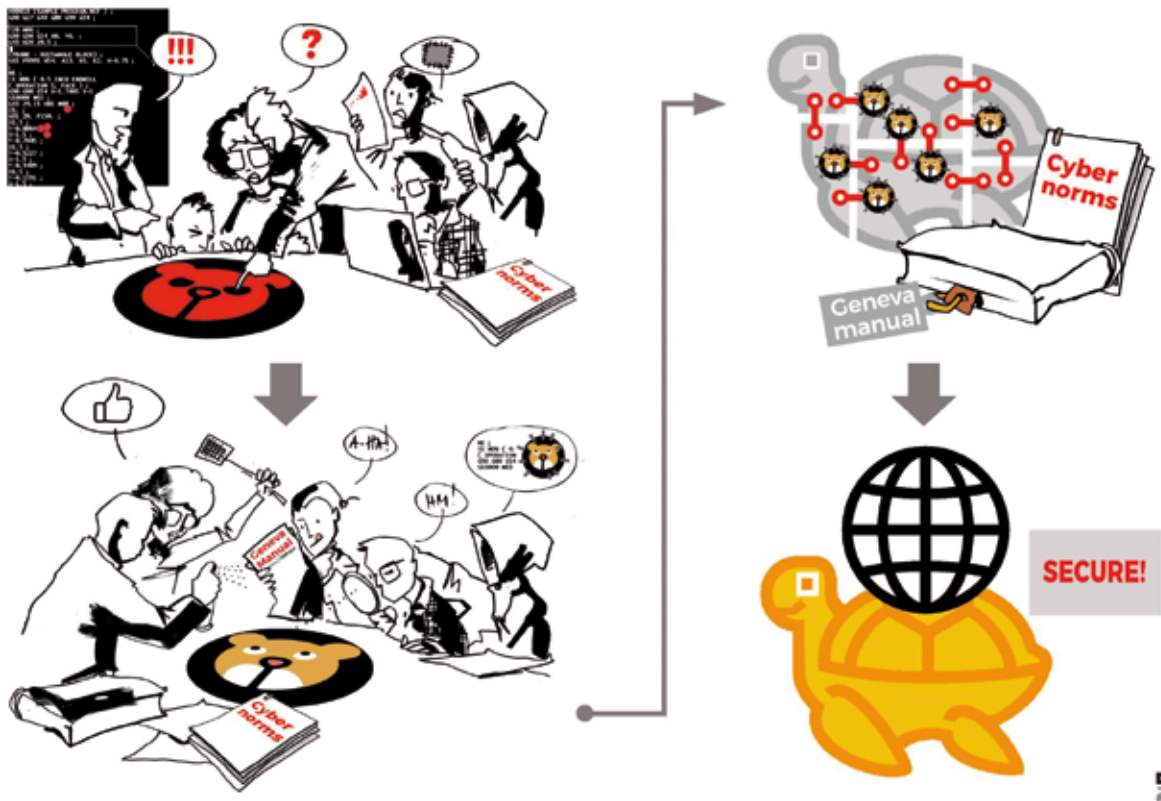
Meanwhile, the use of information and communication technologies (ICT) and *digital products* can be abused by other actors for malicious purposes. This raises security concerns at various levels – from the security of particular users, to matters of international peace and security. States carry primary responsibility for security of its citizens and infrastructure; however, this responsibility is not absolute, as it is clear that they cannot meet these expectations about cyberspace without engaging with other actors: a cooperation between states, private sector, academia, civil society, and technical community is required to ensure an open, secure, accessible, and peaceful cyberspace.



How can non-state stakeholders support states in the implementation of the agreed UN cyber norms and CBMs? Which responsibility do they have and which contribution can they make to address cyber risks and promote responsible behaviour in cyberspace?

The Geneva Dialogue on Responsible Behaviour in Cyberspace (Geneva Dialogue) was established by the Swiss Federal Department of Foreign Affairs and led by DiploFoundation with the support of the Republic and State of Geneva, Center for Digital Trust (C4DT) at EPFL, Swisscom, and UBS to map the roles and responsibilities of various actors in ensuring the security and stability of cyberspace. The Geneva Dialogue stems from the principle of ‘shared responsibility’ and focuses on the **implementation of the agreed UN cyber norms by relevant non-state stakeholders as a means to contribute to international security and peace.**

Concretely, the Geneva Dialogue organises regular consultations to discuss stakeholders’ agreements and disagreements on the interpretation and implementation of the agreed norms and CBMs, while gathering good practices that can inspire the broader international community. Representatives from four stakeholder groups – private sector, academia, civil society, and the technical community (including the open-source community) from all over the world – actively participate in these regular discussions as *Geneva Dialogue experts*.



These findings are published in the [Geneva Manual on Responsible Behaviour in Cyberspace](#) and offer possible guidance for the international community in advancing the implementation of the agreed norms and establishing good practices. The Geneva Manual offers a multistakeholder perspective on these issues and highlights several open questions to which the Dialogue and international community have yet to provide answers, but which are important for states to better understand the challenges they face.

The inaugural chapter of the Geneva Manual focuses on two UN GGE norms: supply chain security and the responsible reporting of ICT vulnerabilities. The second chapter provides an outlook on three additional UN GGE norms and several confidence-building measures (CBMs) aimed at protecting critical infrastructure.

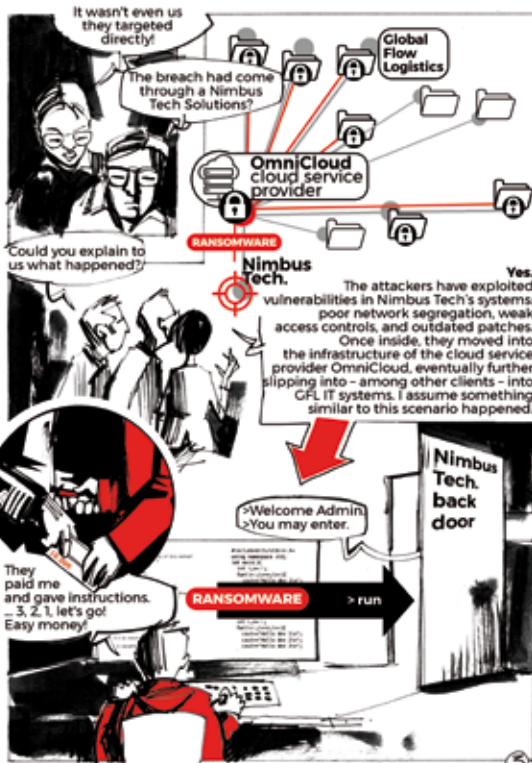
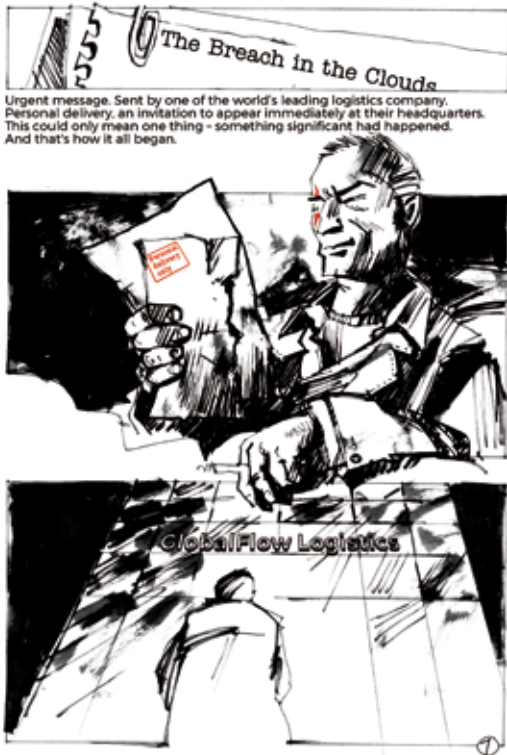
The Geneva Manual offers an action-oriented approach to cyber stability: it explores the roles (Who), responsibilities and actions (What), and challenges. We also connect actions to norms: in sharing stakeholders' interpretations of the norms and drawing a direct line between practical actions and diplomatic agreements, the Geneva Manual thus facilitates the understanding of the UN cyber-stability framework and its effective implementation by relevant non-state stakeholders.

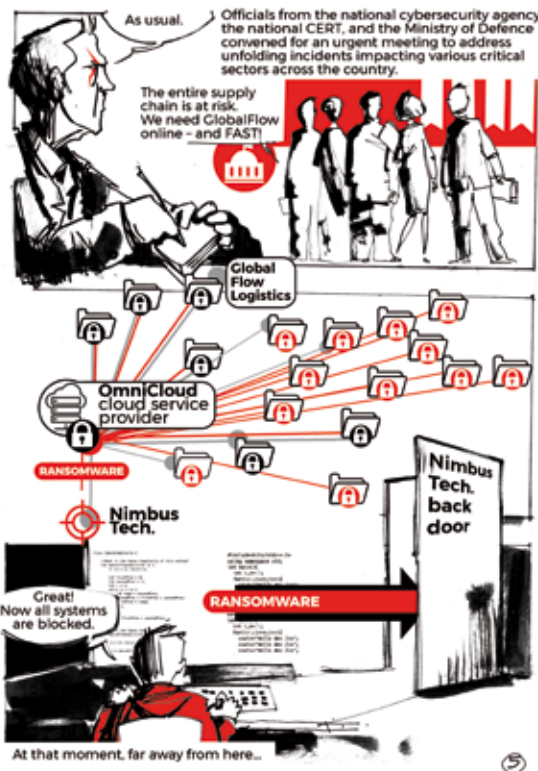
We invite all interested stakeholders to join us on this path to collect ideas, core challenges, opportunities, and good practices to implement the agreed norms and CBMs, and collectively help make cyberspace more secure and stable. The Geneva Manual remains open to comments and suggestions at genevadiologue.ch, and will be continuously updated to reflect the changes driven by the rapid development of technologies.

To access the full version of the Geneva Manual, and contribute to its future editions, visit: genevadiologue.ch/geneva-manual/

HOW DO NORMS GUIDE STAKEHOLDERS IN PROTECTING CRITICAL INFRASTRUCTURE?

Below is a comic book that portrays a fictional story inspired by real events. It highlights the dilemmas that arise when roles and responsibilities among different actors – both domestic and cross-border – are not always clear. The story explores the challenges of addressing cyber risks to critical and critical information infrastructure (CI/CII) and minimising harm while navigating complex multi-stakeholder dynamics.





In this scenario, what actions should different actors have taken to address cyber risks to CI/CII and minimise harm? What guidance do the UN GGE norms offer to stakeholders? These are the questions we discuss in the Geneva Dialogue with the non-state stakeholder experts.

Critical infrastructure (CI) continues to be a consistently attractive target for threat actors and cyber espionage operations.² The vulnerability of critical infrastructure to cyberattacks remains a big concern for cyber defenders both within government and among non-state stakeholders. Despite UN Member States agreeing on cyber norms, with at least three directly focusing on critical infrastructure protection (CIP), many questions remain unanswered regarding strengthening the security of CI and enhancing predictability in this field for all involved actors.

Furthermore, the intensified competitive geopolitical context and the rise of interstate military conflicts, coupled with the rapid exploration and adoption of emerging technologies such as Artificial Intelligence (AI), have brought to light new cyber risks to CIP. These developments have also underscored the complex relationships between public and private actors in managing these risks.

How do approaches to define and protect CI change, in light of the transformative effects of the pandemic and the intensified geopolitical conflicts of the past two years? What guidance do the agreed UN GGE cyber norms and CBMs³ provide to actors in CIP?

From the very beginning, cyberspace has lacked clear delineations between legal concepts and technical systems, resulting in a high degree of interconnectivity and collaboration among actors and communities, leading to uncertainty in their relationships. However, this ambiguity has become even more evident as cyberspace has effectively become a battleground for conflicts,

² Some of the recent cases reported only in 2024: <https://dig.watch/updates/france-faces-unprecedented-cyberattacks-on-government-services>; <https://dig.watch/updates/new-zealand-accuses-china-linked-threat-actors-of-malicious-cyber-activity-targeting-parliament-in-2021> <https://dig.watch/updates/five-eyes-cyber-agencies-attribute-recent-cyberattacks-on-us-critical-infrastructure-to-china-china-refutes-claims>

³ Confidence-building measures (CBMs) are measures designed to prevent misunderstandings and de-escalate tensions when relations among states concerning cyber/ICT security deteriorate. They act as a critical pressure valve to manage and reduce potential conflicts. CBMs emerged during the Cold War with the main goal to address military tensions between adversaries and later evolved as an important instrument to manage crisis situations in international relations. For further details, see ICT4Peace Foundation, 'Confidence Building Measures and International Cybersecurity', 2013, available at https://ict4peace.org/wp-content/uploads/2019/08/ICT-4Peace-2013-Confidence-Building-Measure-And_Intern-Cybersecurity.pdf

posing increasing risks for critical facilities and their users. The significance of aforementioned questions have been underscored during *recent substantive sessions of the UN Open-ended Working Group*, where several states continue to emphasise threats to CI and highlight the need for the development of *practical guidelines for CIP*. Civil society has echoed these concerns, emphasising the importance of *understanding how cyberattacks on CI cause harm to people*. This perspective urges a shift in the discussion from focusing solely on technical aspects to considering the broader societal impacts of such attacks and discussing what is considered as harmful in relation to a cyber incident. Meanwhile, academia has called for a global cyber CIP treaty ‘to make critical infrastructure a cyber attack-free zone and to develop a global accountability mechanism in cyberspace’.⁴

The experts from the Geneva Dialogue (further referred to as ‘experts’) emphasised the importance of discussing relevant CIP norms and highlighted specific challenges arising from the rapid development of information and communication technologies (ICTs). They noted that many critical infrastructure facilities are integrating digital components with legacy systems – some of which were not initially designed for digital use. While legacy systems that are not fully digital may enhance resiliency, the increasing interconnectivity of these systems introduces systemic vulnerabilities and significant cybersecurity risks. This interconnectivity, while potentially improving production efficiency, also comes with added demands for maintenance – not only of hardware, but also of the software used to manage these systems. As a result, some of the efficiency gains are offset by the increased need for software updates and maintenance, further complicating the cybersecurity landscape.

While states play a central role in shaping cyberspace security, they are far from the only actors responsible for its stability. The interconnected nature of modern digital infrastructure means that businesses, software developers, security researchers, and multinational corporations also have significant influence over cybersecurity outcomes. Their decisions – whether to disclose vulnerabilities, patch systems, or comply with regulations – directly impact global security.

Yet, just as states define ‘responsible behavior’ in ways that align with their strategic interests, non-state stakeholders operate under a mix of legal requirements, economic incentives, and corporate policies that shape their approach to responsibility. The discovery of a software vulnerability, for example, presents a company with competing pressures: should it follow national regulations, adhere to internal security policies, protect its shareholders, or act in the best interest of the global community? The answer is rarely straightforward.

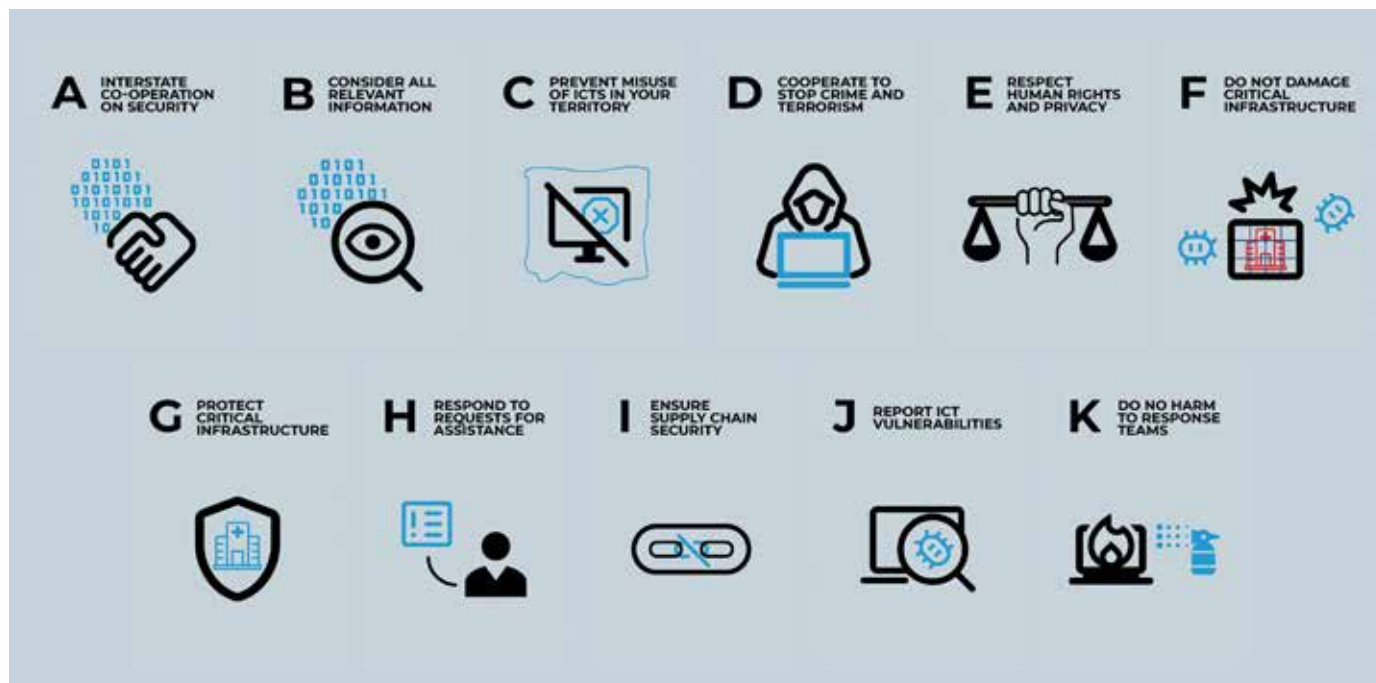
Therefore, in 2024, the Geneva Dialogue initiated discussions on the implementation of agreed cyber norms and CBMs related to CIP. Building on the approach outlined in the *2023 Geneva Manual*, the Geneva Dialogue continued to emphasise the **role of non-state stakeholders in supporting states’ efforts to implement the agreed norms**. Discussions centered on how these stakeholders understand and interpret the norms, the ways in which they can and are already implementing them, the incentives and barriers they encounter, and their expectations from governments. By **highlighting the crucial role non-state stakeholders play in translating diplomatic agreements into practical actions**, the Dialogue emphasises the importance of their involvement. While diplomatic agreements aim to build consensus on a set of actions or best practices, often from a non-CI operator perspective, they can sometimes overlook the context-specific nature of CIP. As such, non-state stakeholders – who possess valuable operational expertise – are often sidelined as mere observers in state-led normative processes, despite their critical role in addressing the nuances of cybersecurity risks.

Although this chapter focuses on non-state stakeholders, it is impossible to separate their actions from the role of governments. State policies on cybersecurity, vulnerability disclosure, and corporate governance shape how companies behave. Even when businesses act independently, they do so within the frameworks set by national regulations and geopolitical pressures. In this chapter, we

⁴ Carnegie Endowment for International Peace, ‘Why the World Needs a New Cyber Treaty for Critical Infrastructure’, March 2024, available at <https://carnegieendowment.org/research/2024/03/why-the-world-needs-a-new-cyber-treaty-for-critical-infrastructure?lang=en¢er=europe>

explore how non-state stakeholders navigate these challenges, examining the factors that shape their decisions and how their 'responsible behavior' intersects with, and at times conflicts with, state interests.

Thus our goal is to offer valuable insights and to spotlight critical, often unanswered, questions that resonate across the cyber diplomacy and cybersecurity communities in both the public and private sectors, contributing to their efforts to reduce cyber risks. Practically, we seek to convey the key perspectives of non-state stakeholders on the implementation of agreed norms related to CIP (i.e. *UN GGE norms F, G, and H*) and to collect examples of effective practices in implementation.



UN GGE norms, DiploFoundation

This chapter should be read in conjunction with the *first chapter*, as the topics of supply chain security (*UN GGE norm I*), responsible vulnerability reporting (*UN GGE norm J*), and CIP (*UN GGE norms F, G, and H*) are interconnected and involve repeating roles and responsibilities for non-state stakeholders. Just as the UN GGE norms are intended to be read collectively rather than separately, the chapters of the Geneva Manual should be considered as a cohesive outcome of the 2023 and 2024 editions of the Geneva Dialogue.

The second chapter is organised as follows:

- Key messages, identified in consultations with non-state stakeholders, on interpretation and implementation of the agreed norms and CBMs related to CIP
- Key roles and responsibilities.
- Annex with the comparative analysis of how states approach CIP and how their approaches have been evolving for the past three–four years (cases of Australia, China, the European Union, Russia, the USA, and Singapore). The analysis, in particular, identifies regulatory trends, enforcement mechanisms, and policy gaps, pointing to areas where non-state stakeholders can drive policy improvements and advocate for more effective multistakeholder engagement. Ultimately, by understanding the trajectory of state-led CIP strategies, non-state stakeholders can proactively contribute to cybersecurity resilience and international cyber stability.

KEY MESSAGES: HOW DO NON-STATE STAKEHOLDERS UNDERSTAND AND INTERPRET THE IMPLEMENTATION OF THE AGREED CIP-RELATED CYBER NORMS AND CBMS?

During regular consultations with experts, we explored the cyber norms and CBMs related to CIP. These discussions covered the implementation of these norms, varying expectations regarding the roles and responsibilities of different actors, and the incentives and barriers they face in reducing cyber risks in accordance with the framework for responsible behaviour in cyberspace. From these conversations, we identified seven key messages. These should not be perceived as a comprehensive list, and as the Geneva Dialogue continues, the list of key findings and messages may expand.

It is important to note that the Geneva Manual does not seek to define critical infrastructure, recognising that each country may prefer its own approach to distinguishing between critical infrastructure (CI), critical information infrastructure (CII), and critical national infrastructure (CNI). The Manual acknowledges these varying definitions and, for the sake of clarity and consistency, uses the term 'critical infrastructure' throughout this document as an umbrella term.

Message #1: More international efforts are required to understand and protect cross-jurisdictional interdependencies in some CI sectors with regional and international impact.

There is no universal approach to defining CI or critical information infrastructure (CII), as each country defines its own CI. Research by the German Council on Foreign Relations (DGAP)⁵ reveals a broader lack of standardised terminology and categorisation for CI and its associated sectors. While the term 'critical infrastructure' is widely used, variations exist, such as 'activities of vital importance' in France or 'crucially important facilities' in Belarus. Indeed, UN Member States have agreed that each '*state determines which infrastructure or sectors it deems critical within its jurisdiction, in accordance with national priorities and methods of categorisation of critical infrastructure*'.⁶ Despite this recognition, many countries still do not maintain comprehensive lists of their CI or CII sectors. According to the DGAP, 94 countries have yet to define their critical infrastructure, highlighting the ongoing challenge of achieving global consistency in CI identification and protection.

Typically, CI is understood to include sectors such as energy, water, transportation, telecommunications and media, healthcare, and finance – those sectors that are directly tied to national security and public safety. However, many assets, systems, and networks within national CI depend on international connectivity (e.g. submarine cables), protocols (e.g. Border Gateway Protocol), and essential services (e.g. Cloud services), which are not necessarily classified as critical at the national level (i.e. supra-national) and, therefore, may lack the same expected level of protection. Recognising this challenge, some governments have begun refining their definitions to account for infrastructure that underpins national security yet operates across borders. For instance, Singapore has introduced⁷ definitions for foundational digital (virtual) infrastructure adjacent to critical infrastructure, acknowledging the role of virtual services and networks that, while not always classified as CI, are crucial for national resilience.

At the same time, some states, such as China and Russia, have adopted the concept of CII rather than CI in their national legal frameworks. However, for simplicity in this document, we will use CI/CII interchangeably throughout the text, as both terms broadly refer to infrastructure essential for national security, economic stability, and public safety. The distinction, however, reflects a broader

⁵Weber, Valentin, Maria Pericàs Riera, and Emma Laumann. 'Mapping the World's Critical Infrastructure Sectors.' DGAP Policy Brief 35 (2023). German Council on Foreign Relations, November 2023, available at <https://doi.org/10.60823/DGAP-23-39548-en>

⁶ UN GGE 2021 report (A/76/135).

⁷ More details are provided in the comparative analysis of certain national legal frameworks for CI/CII protection in [Annex](#).

emphasis on the protection of digital and information systems, including data storage, cloud services, and internet platforms, which these states view as essential to national security and state control. These approaches contrast with traditional CI definitions by prioritising digital resilience and state oversight over physical infrastructure alone. However, despite these national efforts, the broader lack of international coordination to define and secure cross-border interdependencies complicates efforts for CI and CII operators/owners to set clear boundaries for implementing and enforcing security measures and compliance. This results in overlaps and gaps in protection, leaving vulnerabilities and risks for disruption of interconnected systems.

Suggestions for practical actions:

- Relevant stakeholders (CI operators/owners, product vendors and service providers, cybersecurity researchers and incident response experts, open source software (OSS) experts, NGOs and academia engaged in advocacy and research⁸) should assist states in mapping critical interdependencies (i.e. interconnected assets, systems, and networks) between CI sectors. These efforts can be undertaken at the national level, and such contributions from stakeholders can also support states at the regional level and within the UN OEWG.

The efforts could focus on identifying interdependencies related to the technical infrastructure crucial for the general availability and integrity of the Internet. The goal is to pinpoint security challenges and recommend steps to ensure adequate protection of these interconnected assets, systems, and networks against current threats. For instance, the recent faulty CrowdStrike update⁹ underscored complexity and over-reliance/dependence of CI where a lack of security practices unintentionally impacted the availability and integrity of worldwide CI systems and services.

The goal of such mapping should be also an analysis of cause-and-effect relationships and possible cascading failures between such interdependencies.

Contribution to the implementation of:

- Norm G
- Cooperative and transparency UN GGE confidence-building measures



Message #2: Secrecy in defining CI for national security reasons limits the awareness of relevant stakeholders to support states' efforts in CIP.

As it is each country's sovereign right to define its own CI, some countries¹⁰ prefer to keep such a list secret, for national security reasons. Publicly disclosing which organisations are classified as CI could expose them to increased risk of targeted attacks. At the same time, experts highlighted that secrecy over transparency in identification and protection of CI may significantly limit relevant stakeholders' ability to implement the agreed norms and transparency-related CBMs. In particular, DGAP notes that countries that publicly list their CI sectors have not experienced more frequent attacks than those that have yet to define CI. In fact, countries that have codified their CI sectors tend to be more effective in implementing measures to protect critical infrastructure. The European Union's NIS and NIS2 directives serve as examples of regulations that strengthen CI protection. 'Without a definition of CI, protection is not possible.'¹¹

A possible compromise is to adopt a layered approach in which the list of CI entities remains confidential, but general information about the definition of CI, sectors and categories of CI is made publicly available.¹² This layered approach, combined with mechanisms for secure

⁸ For more details, see the discussion on key roles and responsibilities in the next section.

⁹ For an analysis of the cyber failure involving CrowdStrike and Microsoft, see DigWatch, 'Analysis: Cyber failure of CrowdStrike and Microsoft,' published on 19 July 2024, available at <https://dig.watch/updates/analysis-cyber-failure-of-crowdstrike-and-microsoft>

¹⁰ For instance, Singapore: <https://www.csa.gov.sg/faqs/cybersecurity-act> and the US: <https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/>

¹¹ Weber, Valentin, Maria Pericàs Riera, and Emma Laumann. 'Mapping the World's Critical Infrastructure Sectors.' DGAP Policy Brief 35 (2023). German Council on Foreign Relations, November 2023, available at <https://doi.org/10.60823/DGAP-23-39548-en>

¹² For instance, this is how it is done in several countries: the US CISA <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors> and Switzerland <https://www.babs.admin.ch/de/die-kritischen-infrastrukturen> and <https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/c81e27b3-030c-47ed-81cf-ae9409c2572b.pdf>

information sharing among trusted stakeholders, can help strike a balance between transparency and confidentiality.

Additionally, public, non-sensitive research and analysis on sector-specific threats and vulnerabilities, as well as information on national priorities and approaches to secure CI sectors, would provide guidance and help relevant stakeholders improve their security posture and support states' efforts in CIP.

Suggestions for practical actions:

- Relevant stakeholders, including CI operators/owners, product vendors and service providers, as well as NGOs and academia engaged in advocacy and research, should advocate for transparency on a state approach in definition of CI and designation of CI entities and essential services.
- CI operators/owners, product vendors and service providers, as well as NGOs and academia engaged in advocacy and research, can collaborate with governments to help clarify and strengthen the national implementation of agreed cyber norms, ensuring that these norms are effectively communicated and integrated into practice to protect CI.

Contribution to the implementation of:

- Norm G
- Cooperative and transparency UN GGE confidence-building measures



Message #3: The lack of commonly accepted minimum cybersecurity requirements to protect CI results in the limitation of efforts to achieve cyber resilience.

CI across different jurisdictions are highly interconnected and depend on global service providers, such as cloud computing, data centres, and international communication networks (e.g. many CI sectors use shared infrastructure such as fibre-optic cables or communication protocols that span multiple countries; an incident affecting these services can disrupt CI systems across the country or even the region). Commonly accepted and clearly defined minimum security requirements would increase the resilience and protection of CI by contributing to the standardisation of vulnerability handling and threat information sharing, as well as enhancing the effectiveness of incident response. Such requirements should be risk-based and the risk assessments should consider different threats and risks, their likelihood, as well as the existing and potential vulnerabilities. Additionally, such minimum cybersecurity requirements can directly address the UN GGE norms and include standardised templates for requesting assistance in protecting CI, including from relevant stakeholders (e.g. CI operators/owners, incident response community, cybersecurity experts, product vendors and service providers) and responding to such requests.

In addition to these foundational requirements, there is a growing need to focus on raising awareness of software supply chain risks for CI and establishing baseline good practices that specifically address these risks. The *first chapter of the Geneva Manual* highlights the lack of standardised approaches for implementing norm I on ICT supply chain security. Therefore, standardising security practices for the software supply chain, including open source components, can help prevent these widely used tools from becoming weak points in the cybersecurity posture of critical infrastructure. Relevant stakeholders from industry (CI operators/owners, product vendors and service providers, cybersecurity experts) and technical community (including OSS community) could collaborate within Standards Development Organizations (SDOs). Governments can further support this collaboration by encouraging and funding the participation of NGOs,¹³ particularly civil society organisations, which are often underrepresented in SDOs but can offer essential societal perspectives on software supply chain security in the context of CIP.

¹³ 'Government's Role in Increasing Software Supply Chain Security: Toolbox for Policymakers'. Authored by Christina Rupp and Dr. Alexandra Paulus. Interface, 2 March 2023, available at <https://www.interface-eu.org/publications/governments-role-increasing-software-supply-chain-security-toolbox-policy-makers>, accessed January 5, 2025

Suggestions for practical actions:

- Relevant stakeholders, including CI operators/owners, product vendors and service providers, experts from OSS community, should cooperate with policymakers to define commonly accepted baseline cybersecurity requirements and formulate expected end-goals for achieving cyber resilience of CI, particularly where interconnections exist. Given that not all CI sectors are equally interconnected or equally critical, focusing efforts on areas with significant interdependencies could improve the effectiveness of these initiatives and increase the likelihood of achieving meaningful progress in cyber resilience.
- These efforts should also include the harmonisation of regulatory frameworks, including:
 - Incident handling and reporting requirements for CIP and specifically technical infrastructure spanning across national borders
 - Software supply chain security criteria, which also clarify the roles and responsibilities for stakeholders across the software value chain

Contribution to the implementation of:

- Norm G
- Norm H
- Cooperative and transparency
- UN GGE confidence-building measures



Message #4: Obstacles for vulnerability management¹⁴ in industrial control systems (ICS) in the context of CI leave such systems with inherent and unnoticed vulnerabilities creating cybersecurity risks.

ICS in CI sectors, such as energy, chemical, and manufacturing, face unique and complex vulnerability management challenges. These systems are often built on proprietary, closed-source technologies developed by various manufacturers, which can complicate efforts to detect, analyse, and address software vulnerabilities. Unlike traditional IT systems, which may rely on widely used and regularly updated components, ICS systems tend to be specialised, with components that often have long operational lifespans and limited flexibility for modification or updates. As a result, vulnerabilities in ICS may go unnoticed or unaddressed for extended periods, creating cybersecurity risks.

The main challenge in ICS security is patching. While individual components can be tested for vulnerabilities, ICS systems face unique issues. Unlike IT networks, ICS vulnerabilities stem from the need to follow strict safety regulations while keeping operations running smoothly. The integration of ICS with physical processes makes it hard to apply security updates without disrupting operations. Furthermore, safety regulations often focus on maintaining continuity and physical safety, which creates a conflict when trying to apply timely security measures.

Updating or patching ICS components typically requires scheduled maintenance windows, which can sometimes involve temporarily taking the facility offline. While these updates may not always be cybersecurity-related, they are necessary for maintaining system performance and security, and often make financial sense in terms of minimising operational disruptions. However, even during these scheduled maintenance periods, critical infrastructure systems may continue to operate with known vulnerabilities, which may not align with urgent cybersecurity needs. This creates a window of risk where cyber threats could potentially exploit these unpatched vulnerabilities, particularly when the timing of maintenance windows does not coincide with immediate security priorities.

¹⁴ Vulnerability management (VM) involves practices and controls to ensure products are updated with the latest security patches. It covers managing security flaws in both in-house and third-party components, including receiving and analysing vulnerability reports, assessing risks, coordinating mitigation efforts, and issuing security advisories when necessary. For more discussion, see Geneva Dialogue Output Report 'Security of digital products and services: Reducing vulnerabilities and secure design: Good practices', December 2020, available at <https://genevdialogue.ch/wp-content/uploads/Geneva-Dialogue-Industry-Good-Practices-Dec2020.pdf>

ICS components are often proprietary and developed by various vendors, making the process of acquiring and analysing them for vulnerabilities difficult and expensive. Unlike IT systems, where software can be easily downloaded for analysis, accessing ICS components such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs) or other specialised equipment is more challenging due to their high costs, proprietary nature, and limited access to the underlying software. This creates a barrier for independent researchers, slowing down the identification and fixing of vulnerabilities.

Despite these challenges, vulnerabilities in ICS are still identified and disclosed, as demonstrated by *advisories from organisations such as CISA*. These efforts highlight that vulnerability research and responsible disclosure are critical components of strengthening ICS security. However, it is essential for governments, industry stakeholders, and cybersecurity experts to foster a more collaborative environment that encourages research, improves communication between researchers and vendors, and promotes timely updates to reduce risks in ICS networks.

Suggestions for practical actions:

- Relevant stakeholders, including CI operators/owners, product vendors and service providers, experts from OSS community, should cooperate with policymakers to clarify and update legal frameworks governing vulnerability research.
- Moreover, national measures should be implemented to decriminalise vulnerability research and disclosure related to CI within legal boundaries and responsible practices which are recognised by the relevant parties. These practices should be clearly defined and allow for the safe, controlled testing of vulnerabilities in designated environments, ensuring that ethical standards are upheld and safety requirements are met. Governments could play an active role by supporting or facilitating controlled research environments, providing resources, oversight, and collaboration platforms to enable the identification and mitigation of vulnerabilities. This active role could also extend to the establishment of public-private partnerships and funding initiatives that incentivise and support responsible vulnerability research.
- CI operators/owners can also consider specifically building simulators or digital twins for the critical infrastructure to enable cybersecurity research and vulnerability identification without direct implication to online or production systems.
- CI operators/owners, product vendors and service providers, and experts from cybersecurity research and the technical community, including the OSS community, should promote the adoption of security-by-design practices. By integrating security into the design and operation of ICS components, vulnerabilities can be mitigated while ensuring compliance with sector-specific safety requirements.

Contribution to the implementation of:

- Norm G
- Cooperative and transparency
UN GGE confidence-building measures



Message #5: The technical community – such as cybersecurity researchers, incident response experts, and others – finds it increasingly difficult to remain politically neutral, which creates security risks for CIP and securing ICT across different jurisdictions.

The technical community – including cybersecurity researchers, incident response experts, and other specialists – faces increasing challenges in maintaining independence and effectiveness amidst growing geopolitical tensions and restrictions on cross-border cooperation. These challenges create significant security risks for the protection of CI and the securing of ICT systems across jurisdictions.

Rising restrictions on technical cooperation and information exchange, such as those imposed by national security laws,¹⁵ export controls, and geopolitical sanctions, disrupt the ability of experts to collaborate effectively. For example, sanctions on certain countries or restrictions on exporting cybersecurity tools and knowledge can prevent researchers and incident responders from addressing shared threats like ransomware campaigns or state-sponsored attacks. These limitations create operational silos, hinder trust-building, and result in fragmented threat intelligence ecosystems, making it harder to mount a unified defense against sophisticated adversaries.

Increasing restrictions on technical cooperation and information exchange cause discord and impact the work of cybersecurity researchers, incident responders, and other experts who protect cross-border ICT networks and systems. These restrictions limit such communities' exchange of threat information, vulnerability and incident information sharing in the times of complex geopolitical tensions.¹⁶

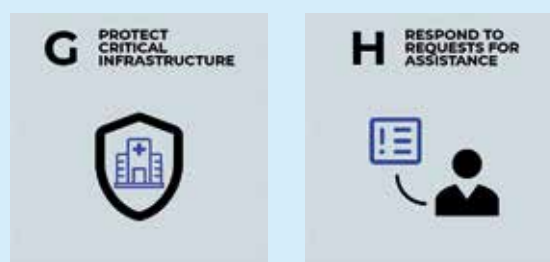
The UN GGE 2015 report in the CBM's section provides¹⁷ that 'States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders', and the third Annual Progress Report in Annex B on CBMs states that the states 'exchange information and best practice on, inter alia, the protection of critical infrastructure (CI) and critical information infrastructure (CII), including through related capacity building'.¹⁸ Geneva Dialogue experts agreed on the significant challenges associated with the cross-border incident and threat information sharing for CIP. The lack of information sharing between states or between relevant stakeholders (e.g. cybersecurity researchers or incident response teams) from different jurisdictions makes it easier for threat actors to exploit vulnerabilities and increases the security risks for all.

Suggestions for practical actions:

- Relevant stakeholders (CI operators/owners, product vendors and service providers, cybersecurity/cyber defence researchers and incident response experts, open source software (OSS) experts, civil society and academia engaged) should advocate for and support policy and legislative measures at the national and international levels to promote effective cooperation among cybersecurity researchers, incident response and security teams, and the open-source community across jurisdictions.
- Such calls could include proposals for the creation of legal provisions in national laws that protect cybersecurity researchers when responsibly disclosing vulnerabilities or engaging in cross-border collaboration, ensuring their actions are not penalised if conducted in good faith and with the intent to enhance security.

Contribution to the implementation of:

- Norm G
- Norm H
- Cooperative and transparency UN GGE confidence-building measures



¹⁵ For instance, see the US Export Administration Regulations (EAR) under 15 C.F.R. §§ 730–774 available at <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-730> and 'Regulations on the Management of Security Vulnerabilities in Network Products', Cyberspace Administration of China (CAC), 2021, available at https://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm

¹⁶ For more discussion, see FIRST Press release on Teams suspension from FIRST, 25 March 2022, available at <https://www.first.org/news-room/releases/20220325> and ZDNet's article on removing Russian maintainers of Linux kernel, 24 October 2024, available at <https://www.zdnet.com/article/why-remove-russian-maintainers-of-linux-kernel-heres-what-torvalds-says>

¹⁷ UN General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 2015, available at <https://dig.watch/resource/un-gge-report-2015-a70174>

¹⁸ A/79/214, July 2024, available at <https://docs.un.org/en/A/79/214>

Message #6: The UN GGE norm F may not fully address the protection of CI, as it primarily focuses on intentional damage, potentially overlooking other scenarios that could affect CI security.

The UN GGE norm F focuses on intentional damage that impairs the use and operation of CI in providing services to the public. However, intentional damage is not limited to physical destruction; it can also include non-physical harms, such as disruptions to systems, economic losses, or psychological and social impacts. Cyber activities targeting or affecting CI frequently result in such non-physical harms,¹⁹ which are not defined as attacks under international law. Moreover, intentional damage may have significant follow-on effects or collateral impacts, such as cascading failures across interconnected systems or long-term societal disruptions. To strengthen protections for CI operators/owners and owners, it is crucial to clarify this norm to address both direct physical harms (e.g., physical damage due to kinetic effects) and indirect harms (e.g. economic disruption, data compromise). Experts further emphasise the importance of defining harm in a comprehensive and measurable manner, supported by evidence-based metrics and data-driven tools.²⁰

Suggestions for practical actions:

- Relevant stakeholders, including CI operators/owners/owners, cybersecurity experts, academia and civil society organisations engaged in advocacy and research, should support States' efforts to clarify definitions of harm (both direct physical and indirect) to broaden the understanding of 'damage' under the norm F. This should include not only physical damage but also harms such as disruptions to digital services, as well as non-intentional or secondary/collateral damage resulting from cyber activities targeting critical infrastructure.
- Relevant stakeholders, including CI operators/owners/owners, cybersecurity experts, academia and civil society organisations engaged in advocacy and research, should support States' efforts to develop international guidelines on how to classify and respond to non-physical cyberattacks on CI and critical services.²¹ The focus of such guidelines should extend beyond physical damage to address harms such as data compromises, service interruptions, prepositioning, and cyber espionage operations, as these activities disrupt critical services and can result in significant societal and economic harm. Emphasising the impact on services rather than solely on infrastructure highlights the real-world consequences for individuals and communities.
- Policymakers, on a national level, should clarify the appropriate government contacts for CI operators/owners/owners to coordinate responses to cyberattacks and prevent escalation in cyberspace.

Contribution to the implementation of:

- Norm F
- Cooperative and transparency UN GGE confidence-building measures



¹⁹'Chinese Cyberattacks on Taiwan Government Averaged 2.4 Million a Day in 2024, Report Says', Reuters, January 6, 2025, available at <https://www.reuters.com/technology/cybersecurity/chinese-cyberattacks-taiwan-government-averaged-24-mln-day-2024-report-says-2025-01-06>

²⁰Statement on Advancing the framework of responsible State behaviour in cyberspace through the Harms Methodology, CyberPeace Institute, 21 March 2024, available at <https://cyberpeaceinstitute.org/news/advancing-responsible-state-behaviour-in-cyberspace-harms-methodology/>

²¹ Experts discussed distinguishing between CI and critical services. CI includes the physical and digital assets, systems, and networks (e.g. power grids, water treatment plants, telecommunications) that enable essential services. Critical services are the essential functions provided by CI, such as electricity, clean water, healthcare, and transportation, which directly impact societal well-being and economic stability. Protecting CI ensures the continued delivery of these critical services, as any disruption to infrastructure can compromise the services people rely on.

Message #7: The increase in inter-state conflicts underscores the need for states to provide clear legal guidance to private entities, helping to protect them and support their efforts in CIP.

Experts had different views on whether a legal distinction between wartime and peacetime is necessary in cyberspace. Some argued that cyberspace has never truly been at peace but has inherently remained a domain of continuous competition, conflict, and contestation. They suggested that such a distinction becomes superficial, as many cyber operations affecting CI fall below the threshold of armed conflict but still cause significant damage.²²

At the same time, other experts underlined that the legal distinction between wartime and peacetime is critical as these are two different legal regimes. Even though UN GGE norms are peacetime norms, there is a distinction between war and non-war from an international law point of view in applicability of the law of war.

Experts also discussed that the distinction between a threat or use of force and an armed attack is critical in determining the appropriate legal response in both physical and cyber domains, and the line between them can be complex, particularly in the context of cyber activities. A 'use of force' refers to actions that may not necessarily trigger a right to self-defence, while an 'armed attack' would justify such a response under international law. The determination of whether an act qualifies as a threat, use of force, or armed attack is to be made by considering all relevant circumstances, including the scale, effects, and intent behind the action. It is important to note that these decisions are rarely confined to the cyber domain alone, as cyber operations often intersect with physical or geopolitical considerations. As cyberattacks increasingly affect CI, the threshold for what constitutes an armed attack in cyberspace should be analysed in the broader context of international law. For instance, the *Tallinn Manual* was cited by experts as an example of comprehensive frameworks for assessing cyber activities against established legal norms.

One of the other concerns is the extent to which governments rely on private-sector entities, often from a foreign state, for IT services and operational support during peacetime, but also in times of crisis and conflict. This engagement can take multiple forms, ranging from direct contractual relationships with defense and intelligence agencies, to more informal cooperation, such as providing cybersecurity assistance, intelligence sharing, or even restricting access to digital services in contested areas.

As these private entities – especially large technology firms – assume critical roles in cybersecurity, their decisions and actions can have geopolitical consequences, sometimes even surpassing the influence of certain states. This raises questions about accountability and governance. The role of industry in modern conflicts has increased and major tech companies 'have evolved into de facto political players, not only by dedicating cybersecurity resources to conflict participants, but also through the ways they – intentionally or otherwise – shape public perceptions of the crisis'.²³ They do so by leveraging powerful cyber intelligence capabilities, such as advanced threat monitoring and analysis, which produce threat intelligence reports that influence the opinions and risk assessments of various actors, including CI owners outside of the conflict zone. To what extent should these private actors be bound by international norms governing responsible state behavior in cyberspace? How does this UN framework of responsible behaviour, including cyber norms translate to private actors' actions in cyberspace during an (armed) conflict?

Compounding this issue is the fact that private actors and civilians today are more likely to become, intentionally or not, involved in armed conflicts²⁴ – whether through cyber operations, digital

²² For instance, Times of India, 'Israel-Hezbollah War: Iran Hit by Massive Cyberattacks, Nuclear Facilities and Government Agencies Targeted', Times of India, 13 October 2024, available at <https://timesofindia.indiatimes.com/technology/tech-news/israel-hezbollah-war-iran-hit-by-massive-cyberattacks-nuclear-facilities-and-government-agencies-targeted/articleshow/114195005.cms> and Industrial Cyber, 'Cyber Attacks Continue to Hit Critical Infrastructure, Exposing Vulnerabilities in Oil, Water, Healthcare Sectors', Industrial Cyber, 14 February 2024, available at <https://industrialcyber.co/critical-infrastructure/cyber-attacks-continue-to-hit-critical-infrastructure-exposing-vulnerabilities-in-oil-water-healthcare-sectors/>

²³ 'Public-private collaboration in Ukraine and beyond', by Taylor Crossman, Monica Kello, James Shires, and Max Smeets. Binding Hook, April 2024: <https://bindinghook.com/articles-binding-edge/public-private-collaboration-in-ukraine-and-beyond/>

²⁴ Several reviewers have noted the Montreux Document, which is primarily addressed to States but also outlines good practices that

platforms, or critical infrastructure – yet their roles and legal status are not always clear. Experts in the Geneva Dialogue have discussed that the agreed UN GGE norms do not create obligations for non-state stakeholders and that it's the responsibility of governments to determine how the agreed cyber norms and international law should be implemented by stakeholders. However, as private-sector involvement in cybersecurity and conflict-related activities grows, there is an urgent need to clarify their responsibilities, particularly for large, influential companies.

At the same time, legal experts note²⁵ that the current geopolitical environment heightens security risks for tech companies, their employees, and users. The International Committee of the Red Cross (ICRC) has outlined *eight rules for 'civilian hackers' during war, and four obligations for states to restrain them*. Notably, the ICRC emphasises that states have a due diligence obligation to prevent violations of international humanitarian law (IHL) by civilian hackers within their territory. However, the reality of cyber operations often disregards territorial boundaries, creating a legal gap in accountability.

Suggestions for practical actions:

- Relevant stakeholders, including CI operators/owners/owners, cybersecurity experts, academia, and civil society organisations engaged in advocacy and research, should cooperate with policymakers to provide legal clarity on responsible behaviour of private actors in cyberspace both during peacetime and conflicts.
- Such stakeholders should also call on policymakers to clarify the lawfulness of using government cyber defence services by CI operators/owners and owners to protect CI.
- Relevant stakeholders should call on policymakers to clarify the appropriate government contacts at a national level for private actors, including CI operators/owners, for a necessary legal guidance to avoid escalation in cyberspace and/or security risks.
- Relevant stakeholders should support States' efforts (e.g. the *Pall Mall Process*) to address the proliferation of cyber intrusion tools as well as an emerging market of commercial cyber defence/offence services.

Contribution to the implementation of:

- Norm F
- Norm G
- Norm H
- Cooperative and transparency UN GGE confidence-building measures



may be valuable for other entities, such as international organisations, NGOs, companies contracting private military and security companies (PMSCs), and the PMSCs themselves. The Montreux Document On pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict, 2008, available at <https://www.montreuxdocument.org/pdf/document/en.pdf>

²⁵Jonathan Horowitz, 'The Business of Battle: The Role of Private Tech in Conflict', Lawfare, August 14, 2020, available at <https://www.lawfaremedia.org/article/the-business-of-battle--the-role-of-private-tech-in-conflict>

KEY ROLES AND RESPONSIBILITIES: HOW CAN NON-STATE STAKEHOLDERS PROTECT CI?

One of the goals of the Geneva Dialogue and Geneva Manual is to break down agreed cyber norms into practical actions that different stakeholders can take to reduce cyber risks. Below is a summary of key roles in implementing CIP-related norms, along with suggested actions – though this is not a comprehensive list.

Role: CI operators/owners

Stakeholder group

The role refers to an entity tasked with managing, maintaining, and securing the assets, systems, and networks designated as critical infrastructure by individual countries. These infrastructures are vital to the functioning of a nation's economy, security, public health, and safety, with each country determining its own criteria for what constitutes critical infrastructure.

These entities may own or control infrastructure across key sectors such as energy, transportation, telecommunications, water supply, healthcare, and financial services.

Actions (responsibilities)

• Risk and continuity management

- **Cyber risk assessment and mitigation strategy:** Conduct regular, in-depth cyber risk assessments tailored to the specific CI systems you manage, considering sector-specific threats, geopolitical risks, and regulatory factors. Use threat intelligence feeds and collaborate with cybersecurity experts to keep assessments up to date. Based on the findings, implement cybersecurity controls suited to each system's risk profile. Ensure security measures are adaptive and scalable to respond to evolving threats.
- **Procurement alignment:** Ensure that the support period for any hardware and software acquired for new or upgraded CI installations is aligned with the product life cycle. For example, avoid acquiring hardware that may be used for 20 years while only receiving software support for 5 years. Establish clear procurement guidelines that require vendors to provide life-cycle support for their products.
- **Cyber-resilience testing and planning:** Regularly test and update business continuity plans to ensure critical CI functions can be maintained during a cyber incident or other emergency. Ensure these plans include contingencies for supply chain disruptions, power outages, and other CI-specific risks.
- **Vulnerability management:** Implement a risk-based approach to vulnerability management by considering asset criticality, network topology, and operational impact. Maintain an up-to-date inventory of all OT assets, including make, model, and firmware versions. Identify communication flows and potential attack vectors. Link asset profiles to known Common Vulnerabilities and Exposures (CVEs) for precise risk assessment. Focus on vulnerabilities that could impact control, visibility, or safety in critical systems. When patching isn't feasible, apply compensating controls such as network segmentation and access restrictions.
- **Incident monitoring:** Use both in-house monitoring tools and outsourced services (e.g. SIEM providers) to detect and respond to cyber threats in real time. Ensure these tools are integrated into your CI's operational environment to provide comprehensive monitoring across OT (Operational Technology) and IT systems.

- **Incident response plan:** Develop and regularly test a tailored incident response plan that includes actionable steps for responding to cyber incidents, including communications protocols, legal reporting procedures, and recovery plans. Update the plan regularly to adapt to emerging threats and vulnerabilities.
- **Stakeholder relationships:** Establish formal and ongoing relationships with relevant stakeholders in the private and public sectors – industry peers, cybersecurity experts and researchers, product vendors and service providers, law enforcement, and government agencies. These relationships should be developed before emergencies arise, allowing for coordinated action when incidents occur.
- **Cybersecurity controls**
 - **Security measures:** Implement cybersecurity technical and organisational measures that are proportionate to the level of risk (e.g. NIST Cybersecurity Framework and IEC 62443 series of standards). Participate in the development and adoption of open standards specific to your CI sector (e.g. IEC 62443 for industrial control systems) to ensure better interoperability and alignment on vulnerability research, threat intelligence, and incident response.
 - **Supply chain security**²⁶: Ensure that components are sourced from manufacturers²⁷ who adhere to best cybersecurity practices, including collaborating with vulnerability researchers, and implementing the recognised standards such as NIST Cybersecurity Framework and IEC 62443 series.
- **Compliance and legal obligations**
 - **Legal guidance for cyber incidents:** Ensure that your organisation understands the legal obligations associated with reporting cyber incidents to national authorities or international organisations, such as CERTs (Computer Emergency Response Teams), and comply with the relevant incident notification laws.
 - **Hacking back restrictions:** Implement strong internal policies and cybersecurity controls that prevent the use of retaliatory cyber operations (hacking back) in the event of an attack. Ensure your legal team is consulted before any action is taken to mitigate attacks.
 - **Legal guidance on the framework of responsible behaviour:** Where applicable, engage with government agencies for clarity on the framework for responsible behaviour in cyberspace, including international law and international humanitarian law (IHL) apply to your CI operations, especially when your infrastructure may be impacted by, or involved in, cross-border conflicts.
 - **Due diligence:** If informed by a legitimate third party (e.g. a CERT), take immediate action to investigate and mitigate any threats or attacks originating from your network. Ensure that threat intelligence sharing agreements are in place with key partners.
- **Education and training**
 - **Employee cybersecurity training:** Conduct regular, targeted cybersecurity training for all employees, focusing on the specific needs and vulnerabilities of the CI systems they interact with.
 - **Framework of responsible behaviour in cyberspace:** Provide regular education to staff and stakeholders on the framework of responsible behavior in cyberspace and relevant aspects of international law and IHL, especially if your CI could be impacted by conflicts.

²⁶ For more discussion on supply chain security responsibilities, see Geneva Manual, chapter 1 on the implementation of the agreed UN GGE norms I and J, 7 December 2023, available at <https://genevdialogue.ch/wp-content/uploads/Geneva-Manual.pdf>

²⁷ For more discussion on supply chain security responsibilities, see role 'Manufacturer and/or supplier of digital products', Geneva Manual, chapter 1 on the implementation of the agreed UN GGE norms I and J, 7 December 2023, available at <https://genevdialogue.ch/wp-content/uploads/Geneva-Manual.pdf>

- **Supply chain and OSS security:** Offer specialised training and resources to employees who manage or use third party components and open-source tools within the organisation, emphasising secure coding practices, vulnerability management, and proper disclosure of security flaws.
- **Collaboration and information sharing**
 - **Cross-sector collaboration:** Join industry working groups, forums, and information-sharing platforms (e.g. ISACs – Information Sharing and Analysis Centers) to exchange threat intelligence and good practices. Establish agreements to share threat data in real-time with trusted partners to improve situational awareness and response coordination.
 - **Vulnerability research partnerships:** Collaborate with cybersecurity experts and researchers to address vulnerabilities in CI systems, including developing proposals to establish clearer legal frameworks that support responsible vulnerability research and disclosure concerning ICS systems.
 - **Public-private collaboration:** Work closely with government agencies and international organisations to shape cybersecurity policies and frameworks that affect your CI sector.
 - **Identification of critical interdependencies:** Work with other CI operators, service providers, and relevant government agencies at a national or international level to identify critical interdependencies between CI sectors and essential services and protocols, including the technical infrastructure essential to the general availability or integrity of the internet.
 - **Response to non-physical cyberattacks on CI:** Contribute to global discussions about the classification and response to non-physical cyberattacks in CI in line with the framework of responsible behaviour.
- **Continuous improvement**
 - **Audit and review process:** Conduct regular security audits of your CI systems and networks, including penetration testing, vulnerability assessments, and threat simulations. Ensure that any gaps identified during audits are addressed promptly.
 - **Feedback and action on audits:** Implement a structured feedback process to ensure that findings from cybersecurity audits and reviews are acted upon across the organisation, with clear responsibilities for follow-up and remediation.
- **Transparency measures:**
 - **Best practices sharing:** Engage with trusted industry peers and government partners to share lessons learned, best practices, and security frameworks that improve CI resilience. Ensure sensitive information is appropriately protected to avoid security risks.
 - **Collaborative risk reduction:** Participate in cross-sector and cross-border initiatives to develop collaborative risk-reduction strategies, aimed at minimising misunderstandings, mitigating conflict risks, and strengthening the overall cybersecurity posture of the CI sector.

Good practices (some examples, but not a comprehensive list)

- [ISA/IEC 62443 Series of Standards](#)
- [NIST Special Publication 800-82 Revision 3 \(NIST SP 800-82r3\)](#) Guide to Operational Technology (OT) Security
- [Guide on the Security by Demand](#): Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products (authored by CISA with contributions from the US government and international partners)

- *ICS Cybersecurity Risk Assessment (ISA)*
- *MITRE ATT&CK for ICS*
- *What private businesses need to know about international humanitarian law by ICRC*
- *Guidance on Principles of OT Cybersecurity for Critical Infrastructure Organisations (International partners)*
- *OpenSSF Open Source Project Security Baseline*
- *Guidance on Improving Security of Open Source Software in Operational Technology and Industrial Control Systems*
- *Operational Technology Cybersecurity Controls and Critical Systems Cybersecurity Controls (Saudi Arabia's National Cybersecurity Authority)*
- *Singapore's Operational Technology Cybersecurity Masterplan 2024 and Codes of Practice*
- *The U.K.'s Cyber Assessment Framework (CAF) for Critical National Infrastructure*
- *Cyber Security Toolkit for boards – Planning your response to cyber incidents*
- *The EU's blueprint to enhance cyber crisis coordination*
- *Collaborative Approach to Eliminating Cyber Security Vulnerabilities, Swiss Cyber Defence Campus*
- *Australia's Executive guidance on Choosing secure and verifiable technologies*
- *Siemens Critical Infrastructure Defense Center*
- *UNIDIR report on Protecting Critical Infrastructure And Services Across Sectors*
- *Cyber Incident Management (CIM) Cybil Portal Resources Guide*
- *Report on Protecting Network Resilience, Network Resilience Coalition (NRC) founded by AT&T Inc., Broadcom, BT Group, Cisco Systems Inc., Fortinet, Intel Corp., Juniper Networks, Lumen Technologies Inc., Palo Alto Networks, Verizon and VMware*

Role: Product vendors and service providers

Stakeholder group

The role refers to an entity that provides essential products, services, or support functions crucial for the operation and security of CI systems. Their products and services are integral to maintaining the functionality, security, confidentiality, integrity, and availability of CI systems.

These entities may include software developers and hardware manufacturers, cloud service providers, telecommunications companies, energy suppliers, maintenance and repair services, cybersecurity firms, and others.

Actions (responsibilities)

• Risk management

- **Risk assessment and management:** Regularly assess and manage risks associated with the ICT products and services you provide, with a particular focus on evaluating the potential impact these solutions may have on the security, integrity, and operational continuity of CI. This includes understanding the specific risks to CI environments and ensuring that your products align with CI protection priorities.
- **Risk mitigation strategies:** Develop and implement tailored risk mitigation strategies that address the unique cybersecurity challenges faced by CI operators. Ensure that the cybersecurity controls embedded within your products and services are designed to minimise threats and vulnerabilities, and are aligned with industry standards (e.g. NIST Cybersecurity Framework, IEC 62443) and best practices to ensure robust protection for CI systems.

- **Cyber-resilience planning:** Ensure the high availability and reliability of your services to support CI operations, including minimising the risk of service disruptions that could affect critical infrastructure. Design your products and services with built-in redundancy, failover mechanisms, and continuous monitoring to maintain operational continuity even during cyber incidents or other disruptions.
- **Cybersecurity controls²⁸**
 - **Security by design practices:** Implement security by design practices in the development of ICT products and services throughout their life cycle and supply chain in line with international standards. Key practices include:
 - Threat modeling to identify and mitigate potential risks early in the design process
 - Avoidance or reduction of common vulnerabilities, such as those outlined in [OWASP Top 10](#), to minimise known security weaknesses
 - Repeatable security testing to continuously validate the security posture of the system throughout its life cycle
 - Design for updates, ensuring that the system can accommodate timely and secure updates, particularly for upstream and open-source dependencies, to address emerging threats
 - **Vulnerability disclosure and coordination:** Implement clear and effective vulnerability disclosure processes that ensure timely response to reports of vulnerabilities. Coordinate actions with relevant stakeholders, including CI operators/owners, cybersecurity researchers, and governmental agencies, to remediate identified vulnerabilities in your products or services. Align your disclosure practices with international standards and norms, such as those outlined by the UN GGE, to support transparency and responsible behaviour in cyberspace.
 - **Vulnerability handling:²⁹** Establish structured vulnerability handling processes to ensure that security patches and updates are applied promptly to address identified vulnerabilities in your ICT products and services. Ensure that these processes are aligned with best practices and the protection of CI, prioritising vulnerabilities that may have the most significant impact on CI security.
 - **Standardised vulnerability exchange:** Use standardised formats for vulnerability exchange, such as the Vulnerability Exploitability eXchange (VEX), to automate and expedite the identification of affected products and allow for faster responses when vulnerabilities are discovered. Ensure that these exchanges are integrated into your operational processes to facilitate swift action on vulnerabilities that could impact CI.
 - **OSS vulnerability communication:** In the event of vulnerabilities discovered in open-source components used in your products or services, immediately communicate with the relevant OSS development teams. Notify them of the discovered vulnerability and any fixes or patches required to mitigate the risk, in line with best practices for responsible vulnerability disclosure.
 - **Data integrity protection:** Implement robust measures to protect data integrity across your products and services. These measures should include preventing unauthorised alterations or tampering of sensitive data, ensuring that data critical to the operation and security of CI remains secure throughout its life cycle.

²⁸ For more discussion on supply chain security responsibilities, see role 'Manufacturer and/or supplier of digital products', Geneva Manual, chapter 1 on the implementation of the agreed UN GGE norms I and J, 7 December 2023, available at <https://genevdialogue.ch/wp-content/uploads/Geneva-Manual.pdf>

²⁹ As defined in the Geneva Dialogue Output report 'Security of digital products and services: Reducing vulnerabilities and secure design: Good practices', p.16, December 2020, available at <https://genevdialogue.ch/wp-content/uploads/Geneva-Dialogue-Industry-Good-Practices-Dec2020.pdf>

- **Supply chain security³⁰**

- **Upstream vulnerability response:** Develop processes for quickly reacting to upstream vulnerabilities, ensuring your products/services do not become entry points for attacks on CI operators' systems.
- **Third-party risk assessments:** Conduct thorough security risk assessments of third-party vendors and suppliers, ensuring they adhere to your cybersecurity standards and minimise supply chain risks.
- **Software Bill of Materials (SBOM):** Maintain and provide upon request a detailed Software Bill of Materials (SBOM) or Hardware Bill of Materials (HBOM) to ensure transparency in the components and dependencies within your products.
- **Collaborative development of security criteria:** Collaborate with other CI operators/owners, product vendors and service providers, cybersecurity experts to develop standardised supply chain security criteria, ensuring that best practices are adopted across the industry.

- **Incident response**

- **Incident monitoring and response:** Implement robust monitoring systems and collaborate with outsourced services (e.g. SIEM providers) to detect and respond to cyber threats in real time. Ensure your products and/or services are seamlessly integrated into the CI environment to provide comprehensive monitoring across IT and OT systems.
- **Incident response plans:** Develop and regularly update incident response plans, tailored specifically for the CI environments you support. Ensure that these plans cover potential cybersecurity events that could affect both your products/services and the CI operators' systems.
- **Notification of security incidents:** Notify CI operators promptly of any significant security incidents or breaches that may impact their critical systems. Work closely with them to provide clear information about the nature of the threat and potential mitigation steps.
- **Coordination with relevant stakeholders:** Actively coordinate with CI operators, industry peers, technical communities, government agencies, law enforcement, and international organisations to share relevant information about incidents. Collaborate on mitigation and resolution efforts to minimise the impact of cyberthreats.

- **Compliance and legal obligations**

- **Compliance with cybersecurity regulations:** Ensure your products and services comply with applicable national and international laws and cybersecurity regulations, specifically those related to CIP.
- **Data protection and privacy laws:** Implement controls to ensure the protection of sensitive data and compliance with data protection and privacy laws, maintaining integrity throughout your services and products.
- **Legal guidance on the framework of responsible behaviour:** Where applicable, engage with government agencies for clarity on the framework for responsible behaviour in cyberspace, including international law and international humanitarian law (IHL) apply to your operations and services, especially when they may be impacted by, or involved in, cross-border conflicts.
- **Due diligence:** If notified by a legitimate third party (e.g. a CERT or CI owner/operator) of threats or attacks originating from your products or services, take immediate and effective action to investigate and mitigate the identified risks.

³⁰ For more discussion on supply chain security responsibilities, see Geneva Manual, chapter 1 on the implementation of the agreed UN GGE norms I and J, 7 December 2023, available at <https://genevdialogue.ch/wp-content/uploads/Geneva-Manual.pdf>

Ensure that you have established threat intelligence sharing agreements with key partners, enabling prompt communication and coordinated efforts to address cybersecurity incidents.

- **Education and training**

- **Employee cybersecurity training:** Ensure regular, comprehensive training for employees on the critical importance of securing critical infrastructure (CI). This should include specific training on implementing cybersecurity controls for CI, understanding how vulnerabilities in products and services can impact CI, and how to manage and respond to those vulnerabilities to prevent potential harm to CI systems.
- **Framework of responsible behaviour in cyberspace:** Provide continuous education to employees and relevant stakeholders on the framework of responsible behaviour in cyberspace, particularly as they relate to the protection of CI. Ensure that employees understand the implications of applicable laws and regulations especially when products and services could be impacted by conflicts. Focus on the UN GGE norms F, G, and H, as well as CBMs and other relevant regional and national normative frameworks, ensuring that all staff are aware of their roles in preventing harmful actions against CI in the context of cyber incidents.
- **Supply chain and OSS security:** Offer specialised training for employees responsible for managing third-party components and open-source tools within the products or services. This training should emphasise secure coding practices, robust vulnerability management, responsible disclosure of security flaws, and the critical importance of supply chain security in the context of CI protection. Encourage compliance with best practices and international standards to ensure the integrity of the CI that relies on your products and services.

- **Collaboration and information sharing**

- **Information sharing with industry and researchers:** Actively collaborate with other CI operators, cybersecurity researchers, and the open-source community to share best practices, threat intelligence, and lessons learned to strengthen overall CI protection.
- **Vulnerability research and disclosure:** Work with cybersecurity experts to identify vulnerabilities in your products and services deployed in CI and ensure responsible disclosure practices are followed, minimising risks to CI environments.
- **Collaboration with government agencies:** Work with relevant government agencies at a national or international level to share information on cyber risks assessments, threats and vulnerabilities, as well as support their efforts in shaping relevant policies and programs.
- **Identification of critical interdependencies:** Work with other CI operators, service providers, and relevant government agencies at a national or international level to identify critical interdependencies between CI sectors and essential services and protocols, including the technical infrastructure essential to the general availability or integrity of the internet.
- **Response to non-physical cyberattacks on CI:** Contribute to global discussions about the classification and response to non-physical cyberattacks in CI in line with the framework of responsible behaviour.

- **Continuous improvement**

- **Audit and review process:** Conduct regular internal audits of your cybersecurity controls to identify weaknesses and areas for improvement. Ensure that these findings are integrated into your risk management processes.

- **Feedback and action on audits:** Implement a structured feedback process to ensure that findings from cybersecurity audits and reviews are acted upon across the organisation, with clear responsibilities for follow-up and remediation.
- **Transparency measures:**
 - **Visibility into security practices:** Provide CI operators with visibility into your security processes, including vulnerability management, data security, and incident history, while ensuring sensitive information is appropriately protected.
 - **Lifecycle security and support:** Clearly communicate the expected product lifecycle during which CI operators can expect security updates and ongoing support for your products.
 - **Collaborative Risk Reduction:** Collaborate with CI operators, industry stakeholders, cybersecurity researchers, and relevant government agencies to discuss methods to reduce cyber risks and address potential vulnerabilities.

Good practices (some examples which complement the good practices of the [Geneva Manual Chapter 1](#), but not a comprehensive list)

- *NIST Special Publication 800-218 on Secure Software Development Framework (SSDF)*
- *NISTIR 8397 Guidelines on Minimum Standards for Developer Verification of Software*
- *Secure By Design: Guidelines (International partners)*
- *Vendor Transparency - NIST Presentation*
- *EU Cyber Resilience Act - Security requirements (Annexes)*
- *ISO/IEC 29147 on Vulnerability disclosure*
- *Supply-chain Levels for Software Artifacts, or SLSA*
- *Guidance on Securing the Software Supply Chain: Recommended Practices for Managing OSS and SBOMs*
- *Product Security Bad Practices*
- *Guide to implementing a coordinated vulnerability disclosure process for open source projects*
- *Advice for organisations on secure OT products*
- *Global Advisory Board on digital threats during conflict (ICRC)*
- *Comprehensive Toolkit for Responsible Technology Use in the Private Security Sector*

Role: Cybersecurity research and incident response experts

Stakeholder group

The role of a cybersecurity researcher refers to a professional who specialises in exploring and analysing various aspects of cybersecurity to identify vulnerabilities, threats, and potential risks in ICT systems, software, and networks.

Incident response experts are specifically responsible for detecting, responding to, and resolving cyber incidents. They work to contain security breaches, mitigate damage, and restore systems.

Actions (responsibilities)

- **Threat intelligence:**
 - **Threat identification:** Proactively identify, assess, and analyse emerging cyberthreats, attack vectors, and vulnerabilities that could directly impact CI sectors.
 - **Predictive models:** Develop predictive models and threat scenarios that reflect the specific risks to CI, using emerging trends, and intelligence to inform CI protection strategies.
 - **Threat intelligence:** Provide timely and actionable threat intelligence to CI operators/owners and relevant stakeholders to enhance early warning systems and mitigate potential risks to CI.
- **Compliance and legal obligations:³¹**
 - **Vulnerability research:** Ensure full compliance with national and international cybersecurity regulations, standards, and guidelines specific to your role in vulnerability and cybersecurity research impacting CI.
 - **Data security:** Adhere to data protection laws and maintain data integrity by implementing controls to prevent unauthorised access, tampering, or leaks of sensitive CI-related data.
 - **Responsible vulnerability disclosure:³²** Investigate cybersecurity vulnerabilities within CI systems, ensuring responsible disclosure by informing system operators or owners first and facilitating remediation efforts.
- **Incident response:**
 - **Expert support:** Provide technical expertise in investigating and mitigating cyber incidents and cyberattacks impacting CI, focusing on understanding attack methods, impacts, and necessary remediation.
 - **Response plans:** Assist CI operators/owners in developing and executing incident response plans, ensuring preparedness to handle potential cyberattacks effectively.
 - **Support during emergencies:** Support incident response teams during live cyberattacks on CI by providing real-time analysis, remediation advice, and lessons learned to reduce the incident's impact.
- **Security solutions development:**
 - **Solution design:** Contribute to the design, development, and deployment of new cybersecurity technologies, tools, and practices to secure CI from emerging and evolving cyber threats.
 - **Continuous improvement:** Continuously evaluate and improve existing cybersecurity controls in response to new vulnerabilities, attack methods, and lessons learned from ongoing cybersecurity research.
 - **Tailored security:** Focus on developing security solutions tailored to the specific needs and vulnerabilities of CI sectors, with an emphasis on resilience, rapid response, and long-term protection of ICS systems.
- **Expertise on CIP:**
 - **CIP expert advice:** Provide expert recommendations to CI operators/owners, government agencies, and policymakers on implementing robust cybersecurity

³¹ For more discussion on supply chain security responsibilities, see role 'Cybersecurity researchers', Geneva Manual, chapter 1 on the implementation of the agreed UN GGE norms I and J, p.37, 7 December 2023, available at <https://genevdialogue.ch/wp-content/uploads/Geneva-Manual.pdf>

³² As defined in the Geneva Dialogue Output report 'Security of digital products and services: Reducing vulnerabilities and secure design: Good practices', p.18, December 2020, available at <https://genevdialogue.ch/wp-content/uploads/Geneva-Dialogue-Industry-Good-Practices-Dec2020.pdf>

controls and processes to secure CI, aligning with best practices and international frameworks.

- **OSS security:** Advocate for and support the development of programs that enhance the security of OSS used within CI environments, ensuring that these tools are effectively protected against vulnerabilities.
- **Vulnerability disclosure:** Advise policymakers on the establishment of government vulnerability disclosure decision processes, ensuring that there are clear, responsible frameworks for addressing discovered vulnerabilities.
- **Vulnerability management:** Work with CI operators/owners and other stakeholders to address challenges for vulnerability research and management in CI systems, including developing proposals to establish clearer legal frameworks that support responsible vulnerability research and disclosure concerning ICS systems.
- **Collaboration and information sharing:**
 - **Cyber drills:** Work closely with CI operators/operators to conduct controlled cybersecurity 'attacks' and simulations (e.g. red team exercises) to identify weaknesses and test the resilience of CI systems.
 - **Incident response plans:** Collaborate with CI operators to design, refine, and update incident response plans, ensuring that both proactive and reactive cybersecurity measures are in place.
 - **Non-proliferation of cyber intrusion tools:** Engage with government agencies, international organisations, private-sector stakeholders, and cybersecurity experts to shape global policies on the non-proliferation of cyber intrusion tools and responsible use of cybersecurity technologies.
 - **Identification of interdependencies:** Work with other CI operators/operators, product vendors and service providers, and government entities at the national and international levels to map and address the interdependencies between CI sectors and essential services, including the technical infrastructure essential to the general availability or integrity of the internet.
 - **Research sharing:** Share research findings, threat intelligence, and actionable insights with CI operators/owners, policymakers, and the broader cybersecurity and cyber diplomacy communities to improve global cybersecurity posture.
 - **Response to non-physical cyberattacks on CI:** Collaborate with stakeholders to support the development of international guidelines on classifying and responding to non-physical cyberattacks on CI, ensuring alignment with the framework of responsible behavior in cyberspace.
- **Training and education:**
 - **Framework of responsible behaviour in cyberspace:** Provide regular training and awareness programs to relevant personnel on the framework of responsible state behavior in cyberspace, and the impact of these frameworks on cybersecurity research.
 - **CI risk training:** Offer training programs on the specific cybersecurity risks associated with CI systems, including how to identify, assess, and mitigate vulnerabilities in accordance with international standards and best practices.

Good practices (some examples which complement the good practices of the *Geneva Manual Chapter 1*, but not a comprehensive list)

- *CERT Guide to Coordinated Vulnerability Disclosure*
- *ISO/IEC 29147:2018 on Vulnerability Disclosure*
- *Belgium's new legal framework for reporting IT vulnerabilities*
- *Incident Response Checklist*
- *CVD policies in the EU*
- *Coordinated Vulnerability Disclosure Process*
- *Cyber Incident Classification: A Report on Emerging Practices within the OSCE region*
- *ASEAN CERT Incident Drill*
- *OAS CSIRT Americas Network*

Role: Open source software (OSS) actors

Stakeholder group

The role refers to an individual, or a group of individuals, who contribute to the development, improvement, and maintenance of OSS projects.³³ This includes the code owners, as well as repositories and organisations that maintain them.

OSS refers to software whose source code is made freely available to the public, allowing anyone to view, modify, and distribute the code.

Actions (responsibilities)

- **Code quality and supply chain security:**
 - **Secure code practices:** Ensure that open source code is developed with high standards of security and is regularly audited for vulnerabilities.
 - **Responsible disclosure:** Follow responsible disclosure practices for vulnerabilities found in OSS, including timely reporting to relevant parties and addressing issues promptly.
 - **Patch development:** Develop and distribute timely patches for known vulnerabilities to prevent exploitation.
 - **Access controls:** Limit who can make changes to the codebase and implement access controls to prevent unauthorised or malicious actors from introducing vulnerabilities in the software.
 - **Role assignment:** Assign roles and permissions to establish accountability for changes to open source projects (especially widely used by CI sectors) to ensure that only vetted contributors can make edits.
 - **Systematic reviews:** Perform systematic code reviews to identify potential security flaws before final release.
- **Collaboration and information sharing:**
 - **Stakeholder collaboration:** Collaborate with CI operators, industry actors, government agencies, and other stakeholders to understand how to enhance the security of open source projects.
 - **Threat intelligence sharing:** Contribute to and participate in threat intelligence sharing platforms that help identify and mitigate emerging threats affecting OSS used in CI.

³³ OSS contributors, developers, and maintainers are used interchangeably in the Geneva Manual.

Good practices (some examples which complement the good practices of the [Geneva Manual Chapter 1](#), but not a comprehensive list)

- [Open source software best practices and supply chain risk management](#)
- [Guide to implement our framework and protect your organisation from the OSS supply chain threats below](#)
- [GitHub Best Practices for OSS Developers working group](#)
- [Securing the open source supply chain: The essential role of CVEs](#)
- [NIST Special Publication 800-218 on Secure Software Development Framework \(SSDF\)](#)
- [Red Hat's open source participation guidelines](#)
- [GitHub Concise Guide for Developing More Secure Software](#)
- [OpenSSF Secure Software Development Fundamentals Courses](#)
- [OpenSSF Best Practices Badge Program](#)
- [LinuxFoundation training course on Secure Software Development: Requirements, Design, and Reuse \(LFD104x\)](#)
- [OSS-Fuzz](#), a free fuzzing-as-a-service platform for popular open source projects
- [Open Source Insights](#) by Google to understand software dependencies
- [OpenSource at Cisco](#)
- [OpenSource projects - Microsoft](#)
- [Huawei Huawei Open Source Release Center](#)
- [Kaspersky Open Source Software Threats Data Feed](#)

Role: Civil society engaged in advocacy, research, training, and communications

Stakeholder group

This role encompasses non-governmental organisations (NGOs), think tanks, academic institutions, advocacy groups, and media entities that actively contribute to enhancing the security and resilience of critical infrastructure (CI). These organisations provide valuable legal expertise by interpreting and explaining the legal frameworks, regulations, and cyber norms applicable to CI protection.

Through research, policy analysis, educational initiatives, and guidance materials, they help CI operators, policymakers, and other stakeholders gain a clearer understanding of their legal responsibilities and obligations.

Additionally, they play a crucial role in public communications by raising awareness, shaping narratives, and fostering informed discussions through media campaigns, investigative journalism, and digital outreach. By engaging with diverse audiences – including industry professionals, policymakers, and the general public – they help bridge knowledge gaps, promote best practices, and drive meaningful dialogue on cybersecurity and resilience in CI.

Actions (responsibilities)

- **Research and analysis:**
 - **Threat impact analysis:** Conduct detailed analyses of cyberthreats targeting CI sectors, focusing on their impact, including societal impact, and cascading effects.
 - **Good practices repository:** Develop and disseminate analyses of best practices for protecting CI, providing actionable insights for common use.
 - **Norms interpretation:** Assist relevant stakeholders, including CI operators/owners, product vendors and service providers, cybersecurity experts and others in interpreting national and international laws related to CIP and ensure clarity on their application to specific contexts.

- **Legislative gaps in CIP:** Identify gaps in national legislation or international legal frameworks where CI protection is insufficient or unclear, and propose solutions to address these gaps.
- **Identification of interdependencies in the cyber domain:** Research interdependencies in the cyber domain between CI sectors across jurisdictions, highlighting potential vulnerabilities and cascading disruptions.
- **Response to non-physical cyberattacks on CI:** Collaborate with other stakeholders to assist policymakers in developing international guidelines to classify and respond to non-physical cyberattacks on CI, aligned with the framework of responsible behavior in cyberspace.
- **Advocacy:**
 - **Guidance on the operationalisation of the framework:** Provide guidance on how international law, including IHL and other international frameworks apply to cyberspace and cyberattacks on CI for relevant stakeholders .
 - **Civilian protection:** Advocate for the protection of civilians by ensuring that CI operators comply with international legal standards and best practices in CIP.
- **Training and capacity building:**
 - **Workshops for stakeholders:** Conduct workshops for policymakers, CI operators/owners, and other stakeholders to improve their understanding of legal obligations related to CIP.
 - **Cybersecurity skills training:** Provide targeted training for professionals in CI sectors, equipping them with the legal and policy skills needed to address and mitigate cyberthreats.
 - **Capacity building:** Organise events to foster collaboration and knowledge-sharing among stakeholders in different sectors and jurisdictions to improve their CIP efforts and, in particular, better understand the operationalisation of the framework of responsible behaviour in cyberspace and its relevance for CIP.
- **Transparency measures:**
 - **Information sharing:** Engage in transparency measures, such as sharing information about practices, lessons learned, and implemented controls, policies and programs related to the protection of CI.
 - **Collaborative dialogues:** Collaborate with CI operators/owners, cybersecurity researchers, relevant government agencies, and international organisations to discuss approaches to reduce cyber risks.

Good practices (some examples which complement the good practices of the [Geneva Manual Chapter 1](#), but not a comprehensive list)

- [A human rights-centered approach to digital public infrastructure](#)
- [Harm methodology](#)
- [Policy brief on Mapping the World's Critical Infrastructure Sectors](#)
- [GFCE Global Good Practices on Critical Information Infrastructure Protection \(CIIP\)](#)
- [Cybil Portal](#)
- [Technology Policy and the Future Role of Stakeholders](#)
- [Comprehensive Toolkit for Responsible Technology Use in the Private Security Sector](#)
- Reports on [Navigating the EU Cybersecurity Policy Ecosystem](#) and [Vulnerability Disclosure: Guiding Governments from Norm to Action](#)
- [UN cyber norms toolkit at ASPI](#)
- [Digital Watch Observatory – OEWG dedicated page](#)

- Analysis on *The Hybrid Role of the Big Tech Companies and the Impact of Courts on the Making of Cyber Norms*

CONCLUSION

The second chapter of the Geneva Manual underscores the essential role of multistakeholder collaboration in implementing the UN GGE norms F, G, and H, as well as CBMs for the protection of CI. It provides concrete, actionable steps for non-state stakeholders to contribute to enhancing CI resilience in the face of an increasingly complex cyber threat environment. The chapter also includes key messages from multistakeholder consultations, provoking further discussion on the interpretation and application of the agreed norms from a non-state stakeholder perspective. These messages could inform policymakers' efforts to protect CI, including within the UN OEWG.

One of the central themes of this chapter is the shared responsibility among states, CI operators and owners, product vendors, service providers, the technical community, including cybersecurity researchers and the open-source software (OSS) community, civil society, and academia. No single entity can tackle the challenges of protecting CI alone. From private-sector ownership to transnational cross-border interdependencies, the complexity of CI requires a collective approach.

The Geneva Manual highlights the critical need for these diverse actors to move beyond observation and take active roles as key contributors to the implementation of the agreed cyber norms and CBMs. Collaboration is not merely an option – it is a necessity to address cyber risks for CI.

This chapter offers practical, targeted recommendations for various stakeholders, promoting the implementation of the UN GGE norms and responsible behaviour in cyberspace. For CI operators and owners, the key message is clear: regular risk assessments, strong supply chain security, and compliance with recognised industry standards are essential to prevent cascading disruptions that could affect multiple sectors across borders.

For product vendors and service providers, the Geneva Manual stresses the need to integrate security by design throughout the product development process. Maintaining software bills of materials and encouraging responsible vulnerability disclosure are crucial for building trust and mitigating risks within CI ecosystems. Additionally, cybersecurity researchers and the OSS community are called upon to uphold high standards in code quality, patch management, and responsible disclosure.

The chapter also highlights a pressing challenge: the lack of sufficient clarity and guidance in today's volatile geopolitical climate, that negatively impacts protection of CI. The ambiguity in the application of the agreed norms and international law to cyberspace leaves CI operators/owners, particularly those in sensitive sectors (e.g. healthcare and energy), exposed to evolving risks that are harder to anticipate or defend against. In addition, non-physical cyberattacks such as data breaches, service disruptions, and ransomware add additional complexity to CI protection. These attacks are often harder to detect, attribute, and mitigate compared to traditional threats, yet their consequences can be severe, affecting the availability, integrity, and confidentiality of CI and critical services. The intangible nature of these harms makes it difficult to quantify the impact, complicating the assessment of risk and the development of effective security measures. Furthermore, these types of attacks can spread quickly across digital networks, amplifying their potential to disrupt multiple sectors simultaneously.

Transnational interdependencies enhance the efficiency of CI across countries, but they also create the risk that a vulnerability or disruption in one system can rapidly cascade and impact others. Different national governance and security standards make coordinating a collective response more difficult. The lack of alignment between policies and the global nature of cyberthreats may delay an effective response to such threats.

Effective CI protection can also be delayed by obstacles such as secrecy which may significantly limit public-private and cross-border collaboration. The Geneva Manual advocates for greater transparency in how policymakers define, understand and approach CI and CI protection – this is important to make sure that relevant stakeholders are informed and meaningfully support such efforts to safeguard CI. All these challenges especially highlight the role of civil society and academia in advancing efforts to protect CI – these organisations are critical in advocating for stronger accountability mechanisms, conducting detailed analyses of threats to CI, including mapping interdependencies between CI in the cyber domain. These stakeholders can also help evaluate legislative gaps, such as a need for clearer legal frameworks that support responsible vulnerability research and disclosure concerning ICS systems. Through their studies, they can assist policymakers, CI operators/owners, product vendors and service providers, and the cybersecurity community in better understanding how the agreed framework of responsible behaviour in cyberspace, including international law and voluntary norms apply to cyber operations affecting CI.

The second chapter of the Geneva Manual is more than a set of recommendations – it is a framework for the multistakeholder collaboration to put the agreed norms into practice. Hopefully, the Geneva Manual serves as a foundation for ongoing refinement and collaboration, ensuring that it remains a flexible resource for addressing emerging challenges. This chapter is also a call for all stakeholders – state and non-state alike – to actively engage in shaping a safer and more resilient cyberspace. By promoting responsible behaviour and collaboration, avoiding further polarization in cyberspace, addressing policy gaps, and committing to shared responsibility, there is a greater hope for more effective responses to the rapidly evolving challenges in protecting CI.

ANNEX

Comparative analysis of how states approach CIP

Executive summary

As cyberthreats grow more sophisticated and geopolitical tensions reshape global security, governments worldwide are expanding their approach to critical infrastructure protection (CIP). From ransomware attacks on energy grids to state-sponsored cyber espionage, threats to essential services—such as finance, healthcare, telecommunications, and supply chains—are more pervasive than ever. In response, countries have broadened their regulatory powers, tightened controls over foreign technology, and imposed mandatory cybersecurity requirements. While the specific governance models and enforcement mechanisms differ, the overall trend is clear: **governments are taking a more assertive role in securing critical infrastructure.**

We have analysed how **Australia, China, the European Union, Russia, Singapore, and the United States approach CIP, examining their strategies over the past 3–4 years.** Our aim is to uncover key lessons to better understand how these states operationalise the UN GGE norms and enhance the protection of critical infrastructure. These countries were selected due to their representation of key actors in the field and their recent efforts to amend legal frameworks in response to external challenges. Our analysis seeks to inform ongoing discussions within the *Geneva Dialogue on Responsible Behaviour in Cyberspace*, particularly concerning the implementation of norms with non-state stakeholders.

Several key observations emerge from this analysis. First of all, whether through expanded intervention powers (Australia), extraterritorial regulatory reach (Singapore), strict data security controls (Russia and China), mandatory cybersecurity obligations (the European Union) and mandatory incident reporting and disclosure obligations (the USA), **nations are reshaping their legal frameworks to address an increasingly complex threat landscape.** As cyberthreats evolve, future CIP strategies will require a balance between regulatory control, technological sovereignty, and cross-border cooperation to ensure national resilience in an interconnected world.

There are other common trends we have observed in how selected jurisdictions – Australia, China, European Union, Russia, Singapore, and the United States – approach CIP. Nearly all governments prioritise supply chain security and impose stricter regulations on foreign technology providers. While the United States, Australia, and the EU take a targeted approach to ban individual companies from adversarial nations, China and Russia aim to go further in achieving supply chain resilience pursuing comprehensive technological self-reliance in CI/CII sectors.

Additionally, nations have also expanded their definition of critical infrastructure or critical information infrastructure, particularly in response to the COVID-19 pandemic and rising geopolitical instability. **Virtual systems of transnational nature** (cloud computing, data centers, globally distributed IT operations) have been widely recognised as integral to national security, leading to expanded regulatory oversight over such services beyond national borders. This trend is also seen in **expanding regulatory powers beyond traditional CI operators to include service providers** (Singapore), **cloud vendors** (all countries), or **manufacturers of digital products and software regardless of whether they are based in a jurisdiction or not** (the EU). In this context, Russia and China have been pioneers imposing strict security obligations, including for overseas companies that provide essential services to their CII, as these countries have long been focusing on regulating data and information security to minimise foreign influence over their data ecosystems and critical infrastructure networks.

A decade ago, many nations relied on voluntary cybersecurity frameworks. Today, they have **moved toward mandatory compliance models, requiring risk assessments, cyber incident reporting, and even mandatory vulnerability reporting** (e.g. the EU and China). Vulnerability management and disclosure processes, supply chain security have been integrated into the list of security obligations for CI operators/owners in all examples analysed below. This reflects a shift toward proactive risk mitigation rather than reactive crisis management. Several states are also similar in their approach to cybersecurity as a core business process, introducing **corporate accountability for executive management** in cybersecurity efforts to achieve cyber-resilience.

The way states define CI or CII reveals their security priorities, governance philosophy, and economic strategy. Some countries, like Australia, define CI broadly to include both physical and digital assets, as well as communication networks and supply chains across 11 sectors, reflecting the interconnected nature of modern infrastructure. In contrast, Singapore focuses primarily on CII, defined as computer systems crucial for delivering essential services. China and Russia also focus on defining CII.

At the same time, despite these advancements in states' effort to operationalise the agreed cyber norms and improve their CIP legal frameworks, there are several areas which, we believe, are missing in analysed approaches to CIP. In particular, there is **a lack of measures for cross-border coordination and intelligence sharing with other jurisdictions**. The EU, due to its intergovernmental nature, is an exception, though even within its framework, information sharing on CI vulnerabilities or incidents with non-EU nations remains limited. Stronger cross-border intelligence-sharing agreements and joint response mechanisms to secure CI that have a cross-border nature or that have a significant impact for several jurisdictions would help address transnational threats, and would contribute to the operationalisation of the agreed confidence-building measures (CBMs).

Additionally, while many countries focus on vendor bans and stricter foreign technology regulations, there is **insufficient emphasis on strengthening supply chain resilience in the context of CIP in a more coordinated regional and global manner**. In particular, securing open-source software and addressing vulnerabilities beyond individual vendors remain overlooked. Current frameworks also place primary responsibility for CIP on private-sector operators, with governments acting as regulatory enforcers rather than active defenders. While Australia has expanded government intervention powers, most national legal frameworks lack sufficient measures or guidance for CIP operators/owners to systematically address cyberattacks at their infrastructure and support them in developing robust defense mechanisms.

Overall, it is important to acknowledge the difficulty in finding evidence of how states integrate these non-binding norms into their policymaking narratives. This keeps the agreed framework largely confined to UN OEWG discussions and, in turn, limits its practical impact. Additionally, there is little transparency on how states operationalise norms and confidence-building measures to secure CI within their domestic policies and in cooperation with other states. This lack of visibility challenges the credibility of the agreed framework, making it more abstract and less effective as a practical tool for international cyber stability.

For non-state stakeholders – including industry players, technology providers, the technical community, civil society, and academia – the key takeaway is the need for deeper collaboration in translating agreed cyber norms into actionable practices. Governments alone cannot guarantee the security of critical infrastructure; a multi-stakeholder approach is essential. As national sovereignty concerns increasingly shape cybersecurity policies, **striking a balance between these priorities and fostering cross-border cooperation** will be critical to developing a resilient and sustainable CIP framework in an interconnected world.

Australia's approach to protect critical infrastructure

Key characteristics

Over the past few years, Australia has expanded and strengthened its approach to CIP in response to evolving cyber and national security threats. Australia eventually moved from a voluntary model to a **centralised, mandatory compliance framework that integrates non-regulatory settings, enhanced cybersecurity obligations, risk management, and government intervention powers**. The main driver behind these changes has been the growing risk posed by state-sponsored cyber actors, ransomware attacks, supply chain vulnerabilities, and the need for stronger national resilience.

Some key characteristics of Australia's evolving approach to critical infrastructure protection over the past five years include the following:

1. Australia takes a **broad and inclusive definition of CI, encompassing a wide range of physical and digital assets**. This reflects Australia's recognition that critical infrastructure is not limited to traditional physical facilities (e.g. power plants, water treatment facilities) but also includes **information technologies, communication networks, and supply chains**. The [Critical Infrastructure Resilience Strategy 2023](#) defines critical infrastructure as those physical facilities, systems, assets, supply chains, information technologies and communication networks which, if destroyed, degraded, compromised or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of Australia as a nation or its states or territories, or affect Australia's ability to conduct national defence and ensure national security.
2. The foundational law – Security of Critical Infrastructure Act 2018 (SOCI Act) was amended in several stages:
 - **In 2021, the Commonwealth Security Legislation Amendment (Critical Infrastructure) Act 2021 (SLACI Act)** broadened the number of sectors captured as CI **from 4 to 11**, including data storage or processing, healthcare and medical, food and grocery, etc. Before, the 2018 SOCI Act only covered electricity, gas, water, and ports. The 2021 SLACI Act also established **mandatory cyber incident reporting**, where critical cybersec incidents must be reported within 12 hours of detection and other incidents – within 72 hours of detection. Moreover, the 2021 SLACI Act **expanded government powers** and specifically granted the Australian government the ability to provide government assistance to state and territory government and CI entities in the event of serious cyberattacks, as well as to **direct operators to take specific actions** to mitigate risks and to **authorise government agencies to step** in and protect CI assets.
 - **In 2022, the Security Legislation Amendment (Critical Infrastructure Protection) Act (SLACIP Act)** further amended the Security of Critical Infrastructure Act 2018 to enact a framework for risk management programs and oblige CI operators to develop and maintain Critical Infrastructure Risk Management Programs (CIRMP). The SLACIP Act also enhanced cybersecurity obligations, **obliging CI operators to understand vulnerability assessments and provide system information to develop and maintain a near real-time threat picture**.
 - **In 2024, the SOCI Amendment (Enhanced Response and Prevention) Act** further expanded the scope and clarified that the SOCI Act **now applies to data storage systems linked to CI**. The 2024 amendments broadened the **government powers to all types of incidents (beyond cyber)**, empowered the regulator to compel a responsible entity to vary its 'risk management program', and integrated telecommunications security regulations from the Telecommunications Act 1997.

3. In addition to the **11 CI sectors**: communications, financial services and markets, data storage or processing, defence industry, higher education and research, energy, food and grocery, healthcare and medical, space technology, transport, water and sewerage; and **22 classes of assets**. Australia distinguishes between industries (i.e. sectors) that are critical to its national security, economy, and social well-being and assets (i.e. specific facilities, systems, or infrastructure within a sector) that are considered critical.
4. Australia's approach relies on **mandatory cybersecurity and risk management obligations, including mandatory incident reporting obligations** (mentioned above). CI operators also must adopt baseline cybersecurity measures. *Systems of National Significance (SoNS)—the most crucial CI assets—are subject to Enhanced Cybersecurity Obligations (ECSO)*, including mandatory cybersecurity exercises, vulnerability assessments, and real-time system reporting.
5. Throughout the years, **Australia favoured expanded government intervention powers** such as action directions, information-gathering directions, and intervention requests, allowing the Government to intervene in CI operations before, during, or after a major cyber incident.
6. Speaking of institutional arrangements, the Cyber and Infrastructure Security Centre (CISC) within the Department of Home Affairs oversees the implementation of Critical Infrastructure Protection (CIP) regulations. Additionally, the Australian Cyber Security Centre (ACSC), operating under the Australian Signals Directorate (ASD), plays a pivotal role in safeguarding critical infrastructure from cyberthreats. The ACSC provides cybersecurity guidance, threat intelligence sharing, and incident response support, working closely with industry and government to enhance resilience against cyberattacks. Australia's national legal framework **balances sector-specific regulations** (e.g. for telecommunications, energy, finance) with a **unified, national approach to CIP governance**, where the 2024 amendments further integrated telecommunications security regulations under the Security of Critical Infrastructure (SOCI) Act, streamlining **cross-sector compliance**. The responsibilities for CIP are split between the Australian government, state and territory governments, and industry, with the ACSC and CISC collaborating to address both cyber and non-cyber risks to critical infrastructure.
7. A key pillar is strong **public-private partnerships**, which is streamlined through non-regulatory settings such as the **Trusted Information Sharing Network (TISN)**. It brings together CI owners and operators, supply chain entities, peak bodies and all levels of government to facilitate information sharing, industry-government engagements, discuss asset vulnerabilities and implement mitigation strategies.
8. Australia puts a special emphasis on **stronger supply chain security and data security measures**. Foreign technology and service providers are now subject to stricter **security reviews**, and the 2024 amendments specifically target high-risk vendors, such as companies linked to adversarial nations.

Key legislation and policies

The cornerstone of Australia's legal framework for CIP consists of several laws and regulations:

- 2018 *Security of Critical Infrastructure Act (SOCI Act)*, amended with the 2021 Commonwealth Security Legislation Amendment (Critical Infrastructure) Act (SLACI Act), the 2022 Security Legislation Amendment (Critical Infrastructure Protection) Act (SLACIP Act), and *2024 SOCI Amendment (Enhanced Response and Prevention) Act* form a foundational framework for CIP in Australia.

- [Telecommunications Sector Security Reforms \(TSSR\)](#) (2018) presents a set of regulatory measures introduced under the Telecommunications Act 1997 to enhance the security and resilience of Australia's telecommunications networks. The TSSR aims to protect these networks from national security risks, including cyberattacks, espionage, and sabotage. Specifically, telecommunications carriers and service providers are required to protect their networks and facilities from unauthorised access and interference.
- The [Critical Infrastructure Resilience Strategy \(2023\)](#) establishes the overarching policy framework that shapes Australia's approach to enhancing critical infrastructure resilience. It sets out three primary objectives to strengthen national security and resilience: (a) enabling infrastructure owners and operators to manage risks and maintain continuity through advanced, risk-based resilience practices; (b) implementing initiatives via robust industry-government partnerships; and (c) bolstering the security and resilience of these stakeholders by providing effective frameworks, tools, and opportunities for improved collaboration.

China's approach to protect critical infrastructure

Key characteristics

China's legal framework for the protection of critical information infrastructure (CII) has evolved significantly in recent years, reflecting a heightened focus on cybersecurity, data security, and national sovereignty. This is also reflected in China's public positions internationally, including within the [UN Open-ended working group](#) where states discuss responsible behaviour in cyberspace and where China specifically emphasises sovereignty and [notes](#) that 'States should exercise jurisdiction over the ICT infrastructure, resources, data as well as ICT-related activities within their territories'.

Over the past few years, China has significantly moved from a reactive and industry-specific framework to a **highly centralised, proactive, and expansive regulatory system**. Unlike the USA and the EU, where industry participation plays a key role in standard-setting and compliance mechanisms for CIIP, China adopts a more state-directed approach, characterised by extensive regulatory oversight across CII sectors. While many CII operators in China are **state-owned enterprises**, which facilitates government involvement, **private entities also contribute to the standard-setting process**, and **standards play a crucial role in the implementation of the legal and regulatory framework**. China's approach emphasises cybersecurity resilience through continuous monitoring, legal obligations such as mandatory cybersecurity reviews, frequent audits, and real-time incident reporting. Compliance is further reinforced by strict penalties for violations, including potential corporate restructuring and financial sanctions, reflecting the government's commitment to centralised regulatory control.

Some key characteristics of China's evolving approach to critical infrastructure protection over the past five years include the following:

1. Central to this framework is the **broad and evolving definition of CII**, referring specifically to 'the important network facilities and information systems', adopts a sector-based approach (prioritising energy and telecom) combined with an impact-based approach (to be considered by 'the protection authorities'). CII are identified by the competent authorities and supervisory authorities per special rules, and the list is subject to adjustments over time. Per the Guiding Opinions of Implementation (MPS 2020), CII includes eligible basic networks, large private networks, core business systems, cloud platforms, big data platforms, the internet of things, industrial control systems, intelligent manufacturing systems, new Internet, emerging communication facilities, and other key objects. The [2021 Security Protection Regulations for CII](#) define critical information infrastructure as important network facilities and information systems within key industries such as public telecommunications, information services, energy, transportation, water conservancy, finance, public services, e-government, and national defense science, technology, and industry. By extending the

scope of CII to cover these new sectors, China ensures that **emerging technologies are integrated into the broader security and resilience framework**, allowing the government to preemptively address potential vulnerabilities before they affect critical national services.

2. **Regulatory oversight** plays a crucial role in China's CIP framework, ensuring that CII operators comply with stringent security measures. The Cyberspace Administration of China (CAC) leads in overall planning and coordination ensuring the overarching protection strategies, while the Ministry of Public Security (MPS), Ministry of Industry and Information Technology (MIIT), and other sector-specific regulators enforce cybersecurity regulations tailored to their respective industries. These authorities are responsible for identifying critical infrastructure within their sectors and ensuring that operators meet the cybersecurity standards set forth in industry-specific rules. The extensive oversight provided by these agencies underscores **China's top-down, centralised approach to CIP**.
3. China places a strong emphasis on **data security**, both domestically and internationally. It is regarded as a core component of national security, ensuring the protection of key industries and government agencies from cyberthreats. The government's focus on data localisation ensures that sensitive information remains within Chinese borders, mitigating risks such as foreign surveillance or economic espionage. By enforcing stringent data handling regulations, China aims to limit foreign companies' influence over its digital economy while simultaneously shaping global data governance standards. Internationally, China leverages its data security policies to assert its position in multilateral forums, such as the *UN Open-Ended Working Group* (OEWG), where it advocates for norms and principles that align with its domestic priorities.

China's **focus on comprehensive data governance** is also seen in a number of stringent laws adopted for the past five years. The *2021 Data Security Law* and the *2024 Network Data Security Management Regulations* play a crucial role in shaping China's data governance framework, particularly by enforcing stricter rules on data localization and the handling of sensitive information. These laws require companies to demonstrate full alignment with national cybersecurity and data protection regulations, ensuring that personal and sensitive information is kept within China's borders. Additionally, the legal framework includes comprehensive monitoring of data flows, including cross-border transfers, which requires companies to undergo government-led security assessments before exporting data. However, the *2024 CAC Provisions on Promoting and Regulating Cross-border Data Flows* reflect an adjustment toward a more balanced regulatory approach, easing certain compliance burdens for CII operators compared to earlier, more stringent requirements. While maintaining the data export compliance system – which includes security assessments, standard contracts, and personal information protection certification – the provisions introduce key exemptions for non-crucial information infrastructure operators providing non-important data to overseas entities. Notably, data exports necessary for fulfilling contracts with individuals, international trade, cross-border manufacturing, and marketing activities are now exempt from pre-review under specific conditions. Additionally, the threshold for mandatory security assessments has been raised, meaning that only data exports involving large volumes of sensitive data or critical information will require such scrutiny. These adjustments alleviate compliance costs for enterprises while still ensuring oversight of high-risk data transfers.

4. Speaking of **obligations for operators of CI/CII**, they are required to establish robust cybersecurity mechanisms to safeguard their systems and data. According to the Security Protection Regulations for CII, operators must establish a robust cybersecurity protection system and a corresponding accountability framework that ensures adequate human, financial, and material resources are allocated to safeguard critical systems (Art. 13). They are also required to create a specialised security management body (Art. 14) responsible for fulfilling specific duties related to risk management and incident response (Art. 15). Regular cybersecurity testing and risk assessments are mandatory, either conducted by the operators themselves or through third-party cybersecurity service agencies (Art. 17). In addition, operators must report significant cybersecurity incidents or threats to both protection authorities and public security authorities (Art. 18) and prioritise security in their supply chains, ensuring that products and services purchased meet stringent safety and reliability standards (Art. 19).

Concerning **data management and security**, CII operators must follow **data localisation obligations** and store personal information and important data collected and generated in China within Chinese territory. CII operators must also draft risk assessment reports detailing the type and amount of important data being handled, the circumstances of the data handling activities, data security risk faced and measures to address them. The 2024 Network Data Security Management Regulations (2024) strengthen data protection requirements further for domestic and international companies. Specifically, the Regulations elaborate on the obligation on organisations to identify any Important Data that they handle and which is generally understood to mean data that, once tampered with, destroyed, leaked, illegally obtained, or illegally used, may endanger China's national security, economic operation, social stability, public health, and safety. If Important Data is identified, organisations must report to the relevant authorities, who will publicly announce and confirm whether such data qualifies as Important Data. If confirmed, in addition to its existing obligations the organisations must conduct risk assessments (and submit them to the CAC and other competent authorities) to include details of cross-border data transfers, verify that contracts effectively bind the recipients to data security obligations and other measures. Large network platforms that process Important Data must also explain in their annual risk assessment reports how they ensure the security of Network Data in their key businesses and supply chains. Network Data Processors must also report any risks from network products or services that endanger national security or public interest to authorities within 24 hours. This is stricter than the previous two-day reporting rule for general security vulnerabilities in network products or services pursuant to the Regulations on the Management of Security Vulnerabilities in Network Products.

5. A key aspect of China's CIP framework is the **graded protection system**, which is central to maintaining cybersecurity across all network operators, including CII operators. As outlined in Art. 21 of the Cybersecurity Law, this system categorises networks into five grades based on the level of security required, which are now enforced through Multi-Level Protection Scheme (MLPS) (and its updated 2.0 version). CII operators are mandated to comply with at least Level III of the graded protection system, ensuring a higher standard of security for critical infrastructure. The graded system addresses both technical and management requirements. On the technical side, operators must ensure secure physical environments, protected communication networks, secure boundaries, safe computing environments, and robust management centers. On the management side, operators must establish safety management institutions, organise safety management teams, assign dedicated personnel to security tasks, and ensure the maintenance of secure facilities (Art. 21). These requirements help standardise security practices across sectors, ensuring a comprehensive approach to protecting critical infrastructure.
6. A critical addition to China's cybersecurity legal landscape is the Regulations on the Management of Security Vulnerabilities in Network Products (2021), which **integrate vulnerability management into the broader CIP framework**. These rules require companies and organisations that identify vulnerabilities in their products to report them to the appropriate authorities before disclosing them publicly. This measure allows China's regulatory bodies to assess the risks associated with the vulnerabilities and take proactive steps to mitigate potential threats before they can be exploited. Network product suppliers, whether domestic or foreign, must also establish internal mechanisms to identify, monitor, and manage vulnerabilities in their products, ensuring that timely fixes and patches are provided. Failure to comply with these reporting requirements could result in penalties, including restrictions on the products or services offered in China's critical sectors.
7. In line with global regulatory practices, the Chinese government has implemented measures to oversee foreign investment in critical sectors, citing national security and the **need for technological self-reliance**. Similar to frameworks such as the *UK's National Security and Investment Act* and the *US Committee on Foreign Investment (CFIUS)*, China imposes restrictions on foreign companies operating in sensitive industries, including energy and critical infrastructure. In some cases, foreign firms are required to establish joint ventures with state-owned enterprises to participate in projects such as power grids or oil

pipelines. Additionally, regulatory frameworks like the Multilevel Protection Scheme (MLPS 2.0) introduce graded security requirements, with stringent localisation obligations that present challenges for foreign companies. Enterprises handling core or important data are also subject to additional oversight, reflecting broader efforts to balance national security concerns with foreign investment regulations rather than a CIIP-specific approach.

Key legislation and policies

The cornerstone of China's legal framework for CIP consists of several laws and regulations:

- *National Security Law* (2015) establishes the foundation for China's national security framework, with Article 25 mandating network and information security measures.
- *Cybersecurity Law* (2017) introduces requirements for the protection of critical information infrastructure (CII), setting obligations for public authorities and CII operators.
- *Multi-Level Protection System (MLPS)* (2019, it has yet to come into force) requires CI operators to classify their infrastructure and application systems into five separate protection levels and fulfill protection obligations accordingly.
- *Cybersecurity Review Measures* (2020, Revised in 2022) focuses on reviewing CI operators' procurement and use of network products and services to mitigate national security risks. According to the 2022 revised measures, foreign companies providing critical technology or network products (e.g. cloud services, communication equipment) must now undergo more thorough cybersecurity reviews before entering or continuing their operations in China. These reviews assess whether their products or services could pose any security risks to national infrastructure. The government evaluates the potential for foreign governments to influence or exploit the products for espionage or cyberattacks.
- *Regulations on the Management of Security Vulnerabilities in Network Products* (2021) provide a framework for identifying, reporting, and addressing vulnerabilities in network products that could pose a risk to China's cybersecurity landscape. The regulations mandate that companies and organisations that discover vulnerabilities in network products must report these flaws to relevant authorities before disclosing them publicly. This is in line with China's broader cybersecurity framework, which aims to control the flow of information regarding security issues and prevent malicious exploitation. Network product suppliers (both domestic and foreign) are responsible for fixing vulnerabilities in their products. If a vulnerability is identified in a product, the supplier is required to provide a patch or security update to address the issue promptly. The regulations specify that network product suppliers must establish internal mechanisms to monitor, identify, and manage security vulnerabilities in their products, as well as implement a process for responding to these vulnerabilities. Public disclosure or exploitation of vulnerabilities is strictly regulated to ensure that sensitive information about potential cyberattack vectors does not leak prematurely, potentially leading to attacks before fixes are implemented.
- *Data Security Law* (2021) establishes strict rules for data protection, classification, and cross-border transfers, further securing national digital assets.
- *Security Protection Regulations for Critical Information Infrastructure* (2021) expands the legal definition of CII, incorporating new technologies such as cloud platforms, AI, and industrial control systems.
- *Network Data Security Management Regulations* (2024, Effective 2025) expands compliance requirements for entities handling domestic and international data. The regulations place new responsibilities on companies operating networks or offering services related to data processing. These companies must ensure they protect both the data they collect and the networks they maintain from cyberthreats. They are required to implement stringent security controls, conduct regular risk assessments, and safeguard personal and critical data from breaches. This means even companies that are not part of critical infrastructure must adhere to the same high standards for data security.

The European Union's approach to protect critical infrastructure

Key characteristics

The European Union (EU) has developed a comprehensive, multi-layered framework for CIP, where the principle of cyber resilience and horizontal internal market instruments are the key to address transboundary threats in a digitalised world. Having recognised an existing regulatory fragmentation, inconsistent resilience across its member states and sectors, and lack of joint crisis response, the EU has introduced several new legal instruments to address these issues in protecting CI.

Some key characteristics of the EU's evolving approach to critical infrastructure protection over the past five years include the following:

1. Recognising the growing interconnectedness of critical sectors, the EU has shifted from a sector-specific model to a **broader cross-sectoral cyber resilience framework**, where interdependencies between sectors become central to resilience planning. This approach also emphasises the need for further **harmonisation** across the EU and the importance of **shared responsibility** between government authorities and private sector operators, requiring critical entities to implement robust security measures, conduct regular risk assessments, and comply with EU-wide regulations.
2. With the adoption of new versions of the *Directive of Critical Entities (CER Directive)* and the, the EU **expanded the scope of critical infrastructure sectors**, where **cybersecurity and resilience measures are now integral to CIP**. These two directives, adopted in December 2022, replaced earlier versions and outdated frameworks and significantly expanded the scope of critical sectors. In particular, the CER Directive broadens the definition of Critical Entities beyond traditional sectors like energy and transport to include digital infrastructure (e.g. cloud computing, data centers, and internet exchange points), financial markets, health, public administration, drinking water, waste management, and space. All CI identified under the CER Directive are subject to NIS obligations. Meanwhile, NIS 2 introduces a two-tier classification for entities and entities are classified based on their importance: essential and important entities (e.g. food supply, manufacturing, postal and courier services, research and education, etc.), where essential entities face stricter requirements due to the critical nature of their services. Important entities have significant impact, but are not as critical.
3. There is **no single agency** solely responsible for CIP and instead there are **multiple regulatory agencies and bodies at both the EU level and the national level**. At the same time, the **EU's institutional structure is highly formalised** and complex. The European Commission plays a central role in shaping and implementing EU policies and legislation related to CIP, and it is the key institution responsible for enforcing EU regulations. The EU Cybersecurity Agency (ENISA) is the key agency for cybersecurity, providing expertise and support to Member States and EU institutions. It also develops *cybersecurity certification frameworks* under the EU Cybersecurity Act. Member States are also directly involved in strategic cooperation and information sharing through the NIS Cooperation Group, which develops best practices and promotes a harmonised approach to cybersecurity across the EU. The CSIRTs Network connects national cybersecurity incident response teams across the EU in sharing threat intelligence and incident response. EU-CyCLONe is a coordination mechanism for managing large-scale cyber incidents at the EU level.
4. **Introduction of strengthened horizontal cybersecurity obligations for operators and service providers, as well as manufacturers of digital products and software** under the NIS2 and *EU Cyber Resilience Act (CRA)*. The NIS2 imposes a risk management approach for companies and provides a minimum list of basic security elements that have to be applied, while the EU CRA, for the first time, introduces a direct accountability for the cybersecurity of digital products and directly mandates manufacturers and developers to ensure products

are secure-by-design and receive long-term security updates among other obligations. Together, these laws create rules that apply across multiple sectors rather than being tailored to specific industries offering a consistent security baseline for all entities in the EU market.

- 5. Integration of supply chain security obligations** for companies by requiring them to address risks in the supply chains and supplier relationship with third-party vendors and service providers. This shift highlights the need for greater accountability among private sector entities in ensuring that vendors and subcontractors meet strict security requirements before their products or services are integrated into critical infrastructure. The NIS2 requires organisations to conduct supply chain risk assessments and ensure vendors comply with cybersecurity standards, while the EU also increased the *foreign direct investment (FDI) screening* restricting high-risk vendors, which is in practice often linked to geopolitical risks.
- 6. Senior management responsibility for ensuring cybersecurity compliance** under the NIS2 shifts responsibility from IT/security teams alone to the highest levels of corporate governance and makes cybersecurity from an IT issue to a business risk. Executives, board members and other C-level management can be held personally liable for failure to implement adequate cybersecurity measures.
- 7. Shift from soft law recommendations to stringent vulnerability management obligations both at the organisational level (NIS2) and at the product level (CRA)** reflects another evolution in the EU's growing recognition that proactive management of vulnerabilities is critical to securing critical infrastructure and digital services. Under the NIS2, organisations are required to assess and address vulnerabilities as part of their overall risk management strategy, and vulnerability management should be part of the cybersecurity policies that companies must establish and maintain. The NIS2 also mandates that entities take appropriate measures to patch known vulnerabilities in a timely manner, especially those that could pose significant risks to the security of services. Meanwhile, the CRA obliges manufacturers to put in place processes for detecting, reporting, and mitigating vulnerabilities in their products, as well as provide ongoing security updates and patches for their products, ensuring that known vulnerabilities are addressed in a timely and systematic manner.
8. The EU also places a strong emphasis on **cross-border threat information/vulnerability sharing and coordination of large scale crises**, acknowledging that threats to critical infrastructure – whether cyber or physical – do not respect national borders and require collective response mechanisms. It is reflected in encouraging coordination within the newly created European Vulnerability Database (EVD), EU-wide vulnerability information sharing through the EU Cybersecurity Agency (ENISA), and national competent authorities. The NIS2 also enhances the role of CSIRTs which are tasked with sharing threat intelligence and incident reports with other Member States' CSIRTs and EU-level entities such as ENISA and CERT-EU. The NIS2 also established the European cyber crisis liaison organisation network (EU-CYCLONe) to support the coordinated management of large-scale cybersecurity incidents and crises at operational level. In addition, the *EU Cyber Solidarity Act* establishes a framework for the EU to offer emergency support to Member States and critical infrastructure operators that are impacted by serious cybersecurity incidents. This could include financial support, technical expertise, and human resources to help countries and organisations respond to and recover from cyberattacks, such as ransomware or advanced persistent threats (APTs).
- 9. Enhanced crisis response and incident reporting** is another novelty in the EU's approach – the NIS2 now requires entities to notify authorities (CSIRT or competent national authorities) about significant incidents (defined by the NIS2) in several stages: (1) without undue delay and in any event within 24 hours of becoming aware of this incident to submit an early warning; (2) without undue delay and in any event within 72 hours of becoming aware of the significant incident, the entity submits an incident notification; (3) upon the request of a CSIRT or, where applicable, the competent authority, the entity submits an intermediate report; (4) not later than one month after the submission of the incident notification under point 2, the entity submits a final report; and (5) in the event of an ongoing incident at the time of the submission of the final report, the entity concerned submits a progress report and then, within one month of the handling of the incident, a final report.

Key legislation and policies

The cornerstone of the EU's legal framework for CIP consists of several laws and policies:

- [Directive on the Resilience of Critical Entities](#) (CER Directive) (2008, Revised in 2022) expands the scope of critical infrastructure sectors and mandates resilience measures for Critical Entities (CEs) across energy, transport, health, finance, digital infrastructure, and more.
- [NIS2 Directive](#) (2022, Replace the 2016 NIS Directive) strengthens cybersecurity requirements for operators of important and essential entities, as well as enhances cross-border cooperation through mechanisms like the CSIRTs Network and EU-CyCLONe.
- [EU Cybersecurity Act \(2019\)](#) introduces EU-wide Cybersecurity Certification Framework for ICT products, services, and processes, and strengthens the role of the European Union Agency for Cybersecurity (ENISA).
- [EU Cyber Resilience Act](#) (2022) introduces cybersecurity obligations for manufacturers of products that contain a digital component, requiring them and retailers to ensure cybersecurity throughout the lifecycle of their products.
- [EU Cyber Solidarity Act](#) (2024) strengthens capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks. The Act includes a European Cybersecurity Alert System, made of Security Operation Centres interconnected across the EU, and a comprehensive Cybersecurity Emergency Mechanism to improve the EU's cyber resilience.

Russia's approach to protect critical infrastructure

Key characteristics

Russia's approach to CIP is intertwined with its strategic objectives of cyber sovereignty, self-reliance, and geopolitical influence. The country has placed a strong emphasis on safeguarding its critical infrastructure as part of its national security strategy, especially in the context of increasingly sophisticated cyberthreats. For the past 3–4 years in response to the evolving threat landscape, particularly following the escalation of the Russia–Ukraine war and the intensified military cyberattacks on CII, Russia has introduced new policies and measures that have updated its approach. These improvements primarily reflect a broader shift towards **self-sufficiency**, **technological independence**, and enhanced **personal accountability** within CII organisations.

Some key characteristics of Russia's evolving approach to critical infrastructure protection over the past five years include the following:

1. At the core of Russia's CIP strategy is the understanding that **data and information are strategic assets in the modern geopolitical landscape**. Russia's **holistic approach** to CIP does not separate **cybersecurity from information security**. Instead, it recognises that **CII systems are not only vulnerable to technical cyberattacks but also to information manipulation and influence operations**. As part of this, Russia's policies explicitly frame **information security and data protection** within the broader context of information security, which is fundamentally tied to its national sovereignty and geopolitical goals. Unlike some Western models that primarily focus on resilience against cyberthreats, Russia integrates **data security, information control, and cyber defense into a single framework**. This reflects the broader Russian concept of 'information security', which extends beyond traditional cybersecurity to include protection from information influence and data sovereignty concerns. Regulations such as [FSTEC Order No. 239](#) establish detailed security requirements for CII operators, including network segmentation, encryption, access control, vulnerability management, and mandatory incident reporting. The [2024 Methodology for Assessing Technical Protection](#) reinforces these principles, ensuring that organisations systematically evaluate their security posture against state-defined criteria.

2. Russia's legal framework **does not provide a clear, standalone definition of CI, but it defines CII and outlines key CII sectors**, such as government, defense, industry (large manufacturing, including atomic and chemical industries), fuel and energy, transport, finance, telecommunications, healthcare, and science (scientific institutions managing critical research data). These sectors are deemed vital for national security and are thus subject to rigorous security standards. **CII organisations are identified** as state bodies and institutions or individual entrepreneurs that own information systems, ICT networks and automated control systems operating in key sectors such as healthcare, energy and banking, as well as organisations that ensure interaction of these systems and networks. CI can be inferred from various laws related to national security, counterterrorism, and emergency response (e.g. *68-FZ (1994) 'On the protection of the Population and Territories from Emergency Situations'* and *35-FZ (2006) 'On Counteracting Terrorism'*). These laws highlight the dual purpose of protecting both the physical and digital aspects of critical infrastructure in the face of external threats, including terrorism and cyberattacks. While the absence of a clear, unified definition of CI may introduce some ambiguity, the broad categorisation of sectors provides a framework that addresses the most sensitive and essential elements of national infrastructure.
3. Russia's approach to CI/CII is characterised by a highly centralised and state-controlled framework that mandates stringent responsibilities for both the government and critical infrastructure organisations. Under *Federal Law No. 187 (FZ 187) on the Security of Critical Information Infrastructure (CII)*, the division of responsibilities for securing critical infrastructure assets is clearly delineated. The law outlines the roles of CII organisations, the Federal Service for Technical and Export Control (FSTEC), and the Federal Security Service (FSB). CII organisations, which include state bodies, institutions, and private entities operating critical sectors such as healthcare, energy, banking, and transportation, are mandated to implement strict security measures to reduce risks to their assets. These organisations must categorise their assets, report to the FSTEC, and comply with regulations aimed at enhancing resilience against cyberthreats. This hierarchical structure ensures a robust and coordinated approach to CIP, with the **FSB and FSTEC playing central roles in oversight and enforcement**.
4. The FSTEC, which operates under the Ministry of Defence, is responsible for maintaining a register of CII assets and investigating vulnerabilities within the software and equipment used by these organisations. This body plays a key role in ensuring that security measures are applied consistently across the CII sectors. The law mandates CII organisations to adopt specific security measures to protect against cyberthreats, with further specifications outlined in various orders such as the *FSTEC Order No. 239* and *FSTEC Order No. 235*. These orders dictate the security requirements for developing systems used within CII organisations and for protecting sensitive data processed by automated control systems (ACS) or industrial control systems (ICS/SCADA). This regulatory environment ensures that Russia's critical infrastructure is protected by **comprehensive, standardised cybersecurity frameworks**, minimising vulnerabilities and the risk of cyberattacks.
5. Through standardisation of vulnerability management practices, i.e. *the guidelines on vulnerability management by the FSTEC* (2023), Russia integrates **vulnerability management and supply chain security into broader CIP efforts**. The guidelines also emphasise the importance of assessing vulnerabilities in third-party software and hardware, reducing the risks associated with supply chain attacks. The FSTEC 2023 guidelines also make a further significant step in **standardising cybersecurity practices** and systemic approach to vulnerability management and disclosure by providing a detailed framework and **aligning de facto with international good practices**. It highlights the need to integrate vulnerability management and ICT supply chain security into security policies to ensure that this is not treated as an isolated task but rather as part of a comprehensive security framework. The guidelines prescribe: (a) monitoring of vulnerabilities and an assessment of their importance; (b) assessments of threat criticality; (c) determination of methods and priorities for vulnerability remediation, such as software updates and the application of other information protection measures; and (d) mitigation of vulnerabilities and assessment of mitigation processes. The

guidelines do also clearly speak about roles and responsibilities clarifying which members of a CII organisation should be involved at each stage of the process. They set out recommended mitigation timelines of 24 hours for critical risk scenarios, seven days for high-risk scenarios, four weeks for medium-risk scenarios and four months for low-risk scenarios.

6. Speaking of **security requirements**, Russia introduced the Technical Specification for Infrastructure Security Assessment in June 2022, which sought to standardise security practices for CII organisations. This specification laid out **clear protocols** for assessing the security posture of CII assets, fostering a more **proactive risk management approach**. Regular security assessments are now mandated to identify vulnerabilities before they can be exploited by **malicious actors**. This approach aligns with international best practices, however while Russia's specifications may reflect the international frameworks, they do not directly reference them, opting instead for **nationally developed practices** designed to suit national security concerns.
7. The Technical Specification also strengthens the **accountability of cybersecurity service providers** by requiring them to hold a **specialised license** and mandating that CII organisations employ a sufficient number of cybersecurity specialists to ensure effective monitoring and defense. Specifically, each organisation must deploy at least 20 cybersecurity experts, including 3 information security architects, to monitor and secure the systems. This emphasis on increasing the quantity and quality of cybersecurity staff indicates Russia's intention to enhance the accountability and quality of the cybersecurity workforce and ensure that CII organisations have the capacity to respond to the growing cyberthreats. The specification not only outlines **specific roles and responsibilities but also integrates a risk-based approach to cybersecurity**, which mirrors international practices aimed at identifying and mitigating threats in a timely manner.
8. Russia focuses on state control over critical infrastructure data, emphasising **data localisation**, and stringent regulations to secure national assets from foreign influence or attack. It mandates that organisations report data and assets to national authorities such as the FSB, reflecting a centralised and state-driven approach to data security. The FSB's 2023 Information Security Monitoring Order mandates CII organisations to report the domain names and external network addresses of all their resources. This move places greater government control over how CII organisations handle and secure their data, ensuring that sensitive information is closely monitored and that potential risks are detected early. The [FSTEC's 2024 Assessment of Technical Information Protection and CII Security Methodology](#) suggests a framework for assessing the level of protection of CII assets in state organisations and CII bodies, and of compliance with minimum requirements for protection against typical information security threats. The results of such an assessment can be provided to the FSTEC voluntarily, however the FSTEC can request an assessment must be reported within 30 days.
9. A significant aspect of Russia's approach to CIP is its emphasis on **incident response and reporting**. Under [FSB Order No. 282](#) (2019), CII organisations are required to report cybersecurity incidents within strict timeframes. CII entities must inform FSB immediately and not later than 3 hours upon detecting a computer incident related to the functioning of a significant CII asset, and within 24 hours with regard to other CII assets. This rapid reporting requirement ensures that the FSB can quickly coordinate responses to mitigate the impact of cyberattacks. The National Coordination Center for Computer Incidents (NCIRCC), reporting to the FSB, is tasked with overseeing incident response, coordinating efforts, and ensuring that CII organisations follow proper protocols. The NCIRCC also conducts regular security assessments of CII assets, ensuring that organisations maintain high levels of security and are prepared for potential cyber incidents.
10. A central feature of Russia's CIP strategy is its push for **national self-sufficiency**, particularly in the context of cybersecurity. The [2022 Presidential Decree](#), which mandates the use of domestic software in CII facilities by January 2025, reflects this drive for technological independence. The law forbids the use of foreign software in critical infrastructure sectors and requires that all CII organisations establish dedicated information security departments. This measure is a clear response to the growing risks associated with reliance on foreign technologies, especially in the wake of geopolitical tensions and the increasing use of

cyberattacks in military conflict. The decision to prioritise **domestic software solutions** reflects a strategic shift aimed at reducing external dependencies, enhancing **cyber sovereignty**, and mitigating the risk of **foreign influence or interference** in Russia's CII. By making CII organisations rely on homegrown technologies, the government seeks to safeguard sensitive infrastructure from potential backdoor access, espionage, or disruptions due to foreign sanctions or cyberattacks. This move towards **technological independence** also supports Russia's broader goal of reducing vulnerabilities in its national security architecture, reinforcing its **national sovereignty** in cyberspace, and ensuring greater **control** over its digital ecosystem.

11. Additionally, the [2022 Presidential Decree](#) further enhanced the governance framework for **CII security** by requiring all CII organisations to establish an **information security department** and making the **heads of these organisations personally responsible** for ensuring the security of CII assets. This shift places **direct accountability on organisational leaders**, signaling a critical move to embed cybersecurity as a core responsibility within organisational management. Rather than relegating cybersecurity to technical departments, this move emphasises its importance at the highest levels of management. By making organisational heads personally liable for cybersecurity, Russia is signaling that CII security is not a secondary concern but a fundamental aspect of running a secure, resilient, and sovereign organisation. This is an important cultural shift towards enhanced accountability and an effort to ensure that cybersecurity becomes a strategic priority across all sectors, from public institutions to private enterprises.
12. The regulatory environment governing CIP in Russia is marked by **a focus on regulatory control, preventative security measures, and real-time monitoring** of CII assets as part of a broader strategy to safeguard national security and prevent cyberthreats. The FSB's 2023 Information Security Monitoring Order mandates that CII organisations report specific technical details about their information systems, such as domain names and external network addresses. This requirement ensures that the FSB has comprehensive oversight of the networks and systems used by critical infrastructure organisations. The FSB is empowered to monitor and enforce compliance with these reporting obligations, strengthening the state's ability to detect vulnerabilities and respond to potential incidents. The GosSOPKA (State System for Detection, Prevention, and Liquidation of Consequences of Computer Attacks), which reports to the FSB, is tasked with **monitoring networks and systems for cyberattacks and vulnerabilities**. GosSOPKA plays an essential role in preventing cyber incidents across CII sectors by implementing early detection systems and coordinating responses to mitigate the consequences of attacks.

Key legislation and policies

The cornerstone of Russia's legal framework for CIP consists of several laws and policies:

- [Federal Law \(FZ\) no. 187 'On the security of critical information infrastructure of the Russian Federation'](#) (2017) establishes the framework for the protection of critical information infrastructure (CII) in Russia. It defines CII as the systems, networks, and facilities that are essential for the functioning of vital sectors such as energy, transport, healthcare, finance, and telecommunications. The law assigns responsibilities for CII security to both the organisations that own these assets and key state bodies like the FSTEC and FSB. It mandates the implementation of security measures to safeguard these infrastructures from cyberthreats, requiring CII organisations to identify, report, and address vulnerabilities, as well as ensure compliance with national standards for security.
- [The Presidential Decree no.166 on the Technological Independence and the Security of CII](#) (2022) represents a significant step towards ensuring technological independence in Russia's CII sectors. It prohibits the use of foreign software in CII facilities by January 2025, promoting the adoption of domestic technologies to reduce reliance on external sources that might pose cybersecurity risks.

- Technical Specification for Infrastructure Security Assessment by the Digital Ministry (2022) provides a standardised approach for assessing the security of CII systems in Russia. It introduces a more structured framework for regular security assessments and proactive risk management, helping organisations identify vulnerabilities before they can be exploited. The specification includes guidelines for conducting security checks and ensuring that CII assets meet specific requirements for resilience against cyberattacks. Additionally, it strengthens the accountability of cybersecurity specialists, requiring them to hold licenses and mandating the deployment of a dedicated team for continuous security monitoring.
- *Information Security Risk Management Standard, GOST* (2022) outlines the principles and methodologies for managing information security risks in Russian CII. It focuses on the need for systematic identification, evaluation, and mitigation of risks related to information security.
- *Guidelines on vulnerability management by the FSTEC* (2023) provide a structured approach for addressing and managing vulnerabilities in CII systems. The FSTEC outlines clear procedures for vulnerability disclosure, identification, and resolution, encouraging organisations to report vulnerabilities promptly and follow systematic processes for patching or mitigating risks. These guidelines reflect global best practices for vulnerability management.
- *Information Security Monitoring Order no. 367 by the FSB* (2023) mandates CII organisations to report critical security information to the FSB, including details about the domain names and external network addresses of all information resources they own or use. By providing the FSB with comprehensive data on CII networks, the order facilitates more effective threat intelligence and incident response coordination across the national security framework.
- *Order no. 282 'On the Procedure for Informing the FSB of Russia about Computer Incidents, Responding to Them, and Taking Measures to Eliminate the Consequences of Cyberattacks on Significant Objects of the Critical Information Infrastructure of the Russian Federation' by the FSB* (2019) outlines the incident reporting obligations for CII organisations as well as post-incident measures to eliminate the consequences of cyberattacks.
- *Order no. 235 'On the Requirements for the Creation of Security Systems for Significant Objects of the Critical Information Infrastructure of the Russian Federation and Ensuring Their Functioning' by the FSTEC* (2017) establishes mandatory security requirements for significant critical information infrastructure (CII) assets in Russia. The order defines technical, organisational, and procedural requirements for designing and maintaining cybersecurity systems for CII; incident response requirements; and obligations to undergo security assessments and audits. The order also presents a risk-based approach mandating that security measures be tailored according to the criticality of the CII asset.
- *Order no. 239 'On the Requirements for Ensuring the Security of Significant Objects of the Critical Information Infrastructure of the Russian Federation' by the FSTEC* (2017)
- *Assessment of Technical Information Protection and CII Security Methodology, by the FSTEC* (2024) offers a comprehensive framework for assessing the security of CII assets and their technical protection mechanisms. It provides specific guidance for evaluating the effectiveness of security measures, ensuring that CII organisations comply with minimum security requirements to protect against typical cyberthreats. The methodology emphasises ongoing assessments and supports self-reporting by organisations, though the FSTEC can mandate assessments if necessary.

The US approach to protect critical infrastructure

Key characteristics

The protection of CI in the United States has evolved into a robust, multifaceted strategy shaped by the growing complexity of both cyber and physical threats. Initially, the US efforts in CIP were

more fragmented, with each of the 16 designated critical infrastructure sectors having its own oversight and security protocols. Over time, these efforts have become more unified, with a stronger emphasis on **integrating cybersecurity and physical security**, fostering public-private collaboration, and adopting a risk-based approach to resilience. For the past five years or so, the US government introduced new laws, executive orders, national strategies, and regulatory frameworks that have **shifted the country from a largely voluntary model to one incorporating more mandatory requirements and robust enforcement mechanisms**.

The escalating cyberattacks on critical infrastructure (e.g. high-profile ransomware attacks against *Colonial Pipeline* in 2021 and *Kaseya* in 2021) highlighted significant vulnerabilities in the US CI and demonstrated the devastating potential of cyberthreats. In addition, growing recognition of supply chain vulnerabilities – exemplified by incidents like the *SolarWinds hack in 2020* and the *Log4j vulnerability* in 2021 – underscored the need for stronger regulatory frameworks and mandatory incident reporting requirements. These efforts aimed to enhance visibility into cyberattacks and increase corporate accountability for cybersecurity risks. US policymakers also shifted focus toward holding manufacturers and developers of ICTs more accountable for safeguarding national infrastructure, recognising that many security gaps in CI stem from software and hardware supplied by third parties.

Some key characteristics of the US evolving approach to critical infrastructure protection over the past five years include the following:

1. The protection of critical infrastructure in the USA is governed by a **multifaceted and complex legal and policy framework** designed to address both cyber and physical threats. **Initially, the USA favoured more a risk-based sector-specific approach** – the *Presidential Policy Directive 21* (PPD-21, 2013) shifted CI protecting from a reactive to a proactive approach and specifically defined **16 CI sectors, each with a designated sector-specific agency**. It also expanded *Information Sharing and Analysis Centers (ISACs)* to improve sector-specific cyberthreat intelligence, and enhanced coordination between federal agencies, private sector CI operators, and local governments.

However, in recent years, the USA has expanded federal cybersecurity oversight through the adoption of the *National Cybersecurity Strategy (2023)* and *National Security Memorandum-22* (NSM-22, 2024). This marked a **significant shift from a decentralised, sector-specific model to a more centralised federal coordination model**. The Cybersecurity and Infrastructure Security Agency (CISA) was designated as the national coordinator for CI security and resilience, enhancing cross-sector coordination and harmonising risk management efforts across different infrastructure sectors. Sector-specific agencies still exist, but their role was **more integrated under CISA's and DHS leadership under the Biden administration**.

2. The **definition of CI** has changed over time. The first formal federal definition of 'critical infrastructure' was developed in 1996 when President Clinton signed *Executive Order 13010*, where the President outlined that 'certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States'. It becomes a foundation for the current definition – CISA defines critical infrastructure as those infrastructure systems and assets that are so vital that their incapacitation or destruction would have a debilitating effect on security, the economy, public health, public safety, or any combination thereof. This broad definition allows for an inclusive approach to protecting infrastructure in both the public and private sectors, ensuring that all essential services and systems are considered when developing security measures.
3. While the original *16 CI sectors* remain, the scope within those sectors has broadened over the past several years to emphasise cybersecurity, with **increased attention on the interdependencies between sectors**. For example, the Information Technology and Communications sectors have become much more prominent in cybersecurity and national security discussions. The recently adopted laws (as mentioned below) outline a growing recognition that the security of one sector (like energy or transportation) increasingly depends on the integrity of other sectors (like telecommunications and IT).

4. Speaking of **cybersecurity requirements and obligations for CI operators**, the foundational [Executive Order on Improving CI Cybersecurity \(2013\)](#) highlighted the need to develop and implement risk-based standards. This focus on **standardising security practices has become a trend-setting feature** of the US approach, influencing critical infrastructure protection (CIP) efforts in other countries. Notably, the [2013 Executive Order](#) also led to the creation of the [NIST Cybersecurity Framework \(CSF\)](#), which has since become a cornerstone of cybersecurity risk management for CI operators worldwide. Later, the **NIST CSF and its 2024 update became the de facto cybersecurity risk management model for CI operators worldwide**. It provided structured, **voluntary guidelines** organised around the Core Functions: Identify, Protect, Detect, Respond, and Recover. The 2024 update introduced the 'Govern' function, which emphasises **executive accountability for cybersecurity**, further strengthening the framework's focus on leadership and governance.
5. Another critical trend has been the adoption of [Zero Trust Architecture \(ZTA\)](#) as a key cybersecurity standard for federal agencies. The Executive Order 14028 (2021) mandates the implementation of Zero Trust principles across all federal agencies, reflecting a broader shift toward a more robust, proactive defense model. Zero Trust assumes that every network request, whether internal or external, is potentially malicious, requiring continuous validation before granting access. This architecture is increasingly seen as essential for protecting critical systems from sophisticated cyber attacks.
6. The USA has adopted a **hybrid regulatory model for CIP that blends voluntary frameworks with mandatory compliance requirements and emphasises a harmonisation of risk management requirements across CI sectors**. While a significant portion of CI protection is based on voluntary participation and adoption of standards (as mentioned above), especially in the private sector, increasing regulatory demands have pushed for **mandatory cybersecurity requirements**. A lack of mandatory requirements was cited in the [2023 National Cybersecurity Strategy](#) as a factor resulting in inadequate and inconsistent outcomes. Therefore, the strategy set out the strategic objective to establish cybersecurity requirements as well as an initiative on cyber regulatory harmonisation. In setting cybersecurity regulations for CI, policymakers should define **minimum expected cybersecurity practices or outcomes**. The adoption of the [SEC Cybersecurity Rules](#) for public companies and CI operators also reflect this trend, as they introduce **mandatory cybersecurity disclosures, corporate accountability, and a broader market-driven approach to resilience**. This hybrid model provides flexibility for organisations while encouraging them to take proactive steps to secure their systems, balancing between guidance and regulation.
7. The **shift from voluntary to mandatory incident reporting** has also taken place recently. While the [2015 CISA](#) encouraged voluntary sharing of cyberthreat intelligence, the [Cyber Incident Reporting for Critical Infrastructure Act of 2022](#) mandates that CI operators report cyber incidents to the federal government within 72 hours and disclose ransomware payments within 24 hours.
8. The USA has increasingly recognised the critical need to **strengthen supply chain security**, particularly as cyberthreats targeting suppliers and vendors have grown more sophisticated. The [NSM-22](#) and subsequent policies highlight the vulnerabilities in supply chains and call for enhanced protections against cyberthreats that could compromise not only the security of individual organisations but also the resilience of the entire critical infrastructure ecosystem. The [Executive Order 14028](#) (2021) emphasised supply chain security by mandating that federal agencies and contractors adhere to NIST guidelines and adopt cybersecurity best practices. Additionally, the **concept of Software Bill of Materials (SBOM)** was introduced, requiring that federal contractors provide a detailed list of software components used in their products, helping identify potential vulnerabilities and mitigate risks. The US government has also focused on **creating incentives for service providers to implement security-by-design principles**, ensuring that products and services are developed with built-in cybersecurity features. However, unlike the EU Cyber Resilience Act, which establishes mandatory cybersecurity requirements for companies, the US government has opted for a **voluntary soft law approach, avoiding the creation of mandatory federal cybersecurity legislation**.

The US government's commitment to safeguarding its supply chains has been further emphasised through measures like the **National Defense Authorization Act (NDAA, 2017)**, which introduced bans on vendors such as Huawei, ZTE, and Kaspersky due to potential risks to the US national security.

Lastly, as the majority of CI is privately owned in the USA, the government also relies on strong partnerships between federal agencies and industry stakeholders and outlines **public-private partnerships as a core element of CIP efforts**. The National Cybersecurity Strategy and NSM-22 stress the importance of collaboration between the public and private sectors, with an emphasis on sharing cyberthreat intelligence.

Key legislation and policies

The cornerstone of the US legal framework for CIP consists of several laws and policies:

- *The Executive Order 13636 on Improving Critical Infrastructure Cybersecurity* (2013) strengthened the cybersecurity of critical infrastructure in the USA. It directed the establishment of a voluntary framework for cybersecurity risk management and facilitated public-private collaboration to enhance resilience. It led to the creation of the NIST Cybersecurity Framework (CSF).
- *The Presidential Policy Directive 21 (PPD-21) – Critical Infrastructure Security and Resilience* (2013) identified 16 critical infrastructure sectors and emphasised the importance of a coordinated approach between government and private sectors in addressing both cyber and physical threats. It encouraged risk assessments and promoted Information Sharing and Analysis Centers (ISACs) to enhance cybersecurity and resilience.
- *The Federal Information Security Modernization Act* (2014) modernised the Federal Information Security Management Act (FISMA) by improving the protection of federal government information systems. It mandated that federal agencies adopt the NIST Cybersecurity Framework and required them to implement strong cybersecurity controls, including risk assessments and continuous monitoring.
- *The Cybersecurity Information Sharing Act* (2015) encouraged private sector companies to voluntarily share cyberthreat intelligence with the Department of Homeland Security (DHS) to improve collective defense against cyberattacks. It also established legal protections for companies sharing cyber information, enhancing trust between the private sector and government entities.
- *The NIST Cybersecurity Framework (CSF) – First and 2.0 Versions* (2016 and 2024) provided a flexible, risk-based approach to cybersecurity for critical infrastructure sectors. It includes five core functions – Identify, Protect, Detect, Respond, and Recover – and was updated in 2024 (CSF 2.0) to incorporate governance, supply chain risks, and the Zero Trust security model for modern infrastructure.
- *The Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (2017) called for federal agencies to assess and strengthen their cybersecurity practices, improve risk management frameworks, and implement best practices for securing federal IT systems. It also required the modernisation of federal infrastructure to better defend against evolving cyberthreats.
- *The Executive Order 14028 on Improving the Nation's Cybersecurity* (2021) focused on enhancing the US government's cybersecurity posture, including adopting Zero Trust Architecture, improving software supply chain security, and mandating the use of a Software Bill of Materials (SBOM) for federal agencies and contractors. It strengthened the ability of the federal government to respond to and mitigate cyberattacks.
- *The Executive Order 13984 on Supply Chain Security* (2021) aimed at addressing cybersecurity risks within the US supply chain, particularly concerning foreign adversaries. It introduced measures to limit the use of high-risk foreign technology and software (e.g. from China and Russia) in critical infrastructure sectors and federal procurement processes.

- *The Cyber Incident Reporting for Critical Infrastructure Act* (2022) mandated that CI operators report significant cyber incidents to CISA within 72 hours, and ransomware payments within 24 hours. This legislation aims to improve the visibility of cyberthreats and enhance national cybersecurity resilience through timely reporting and response.
- *The National Cybersecurity Strategy* (2023) outlined the US government's approach to securing cyberspace, emphasising the need for stronger protections for critical infrastructure. It shifts accountability toward software vendors, prioritises cybersecurity resilience for CI operators, and promotes public-private collaboration in threat intelligence sharing and incident response.
- *The National Security Memorandum 22* (NSM-22) – National Cybersecurity Strategy for Critical Infrastructure Protection (2024) outlined the US government's approach to enhancing critical infrastructure protection. It centralises federal efforts for securing critical infrastructure, shifting from a sector-specific model to a more coordinated and centralised approach led by the Department of Homeland Security (DHS) and its Cybersecurity and Infrastructure Security Agency (CISA). It emphasises cross-sector collaboration, harmonises risk management efforts across different infrastructure sectors, and strengthens public-private partnerships. The memorandum also prioritises risk mitigation in emerging areas such as supply chain vulnerabilities, cyberthreats from nation-states (e.g. China and Russia), and advanced technologies like AI, alongside the adoption of security-by-design principles and the implementation of baseline resilience measures for CI operators.
- National Defense Authorization Acts (NDAA, multiple years) annually set the budget and policies for the US Department of Defense. Over the years, various versions of the NDAA have included provisions focused on cybersecurity for critical infrastructure. For instance, the 2017 NDAA introduced bans on the use of high-risk foreign technology (e.g. Huawei, ZTE) in federal critical infrastructure procurement, addressing national security concerns related to supply chain vulnerabilities. The NDAA also includes measures to improve cybersecurity standards for both defense and non-defense critical infrastructure sectors, supporting broader national efforts to secure these assets from cyberthreats.
- *The SEC Cybersecurity Rules on Cybersecurity Risk Management for Public Companies* (2023) introduced rules requiring publicly traded companies to enhance their cybersecurity risk management practices. The rules mandate that companies disclose significant cyber risks, incidents, and their cybersecurity strategies to shareholders. Additionally, companies must provide timely updates on material cybersecurity breaches. These regulations emphasise corporate accountability and make cybersecurity a board-level issue, ensuring that companies prioritise cyber risk management and establish clearer transparency for investors regarding their cybersecurity posture.

Singapore's approach to protect critical infrastructure

Key characteristics

Singapore's approach is characterised by a robust legal framework, strong public-private partnerships, and a proactive, risk-based strategy. The cornerstone of this framework is the Cybersecurity Act (2018), which provides a legal basis for the protection of critical information infrastructure (CII) and the associated cyberspace in Singapore. The Act empowers the Cyber Security Agency of Singapore (CSA) to oversee and enforce cybersecurity measures across the critical sectors providing essential services, and additional organisations deemed to be of importance to the nation. The Act has three key objectives to (i) strengthen the cybersecurity posture of important computer systems; (ii) give the Commissioner of Cybersecurity the mandate and powers to prevent and respond to cybersecurity threats and incidents; and (iii) establish a licensing framework to regulate cybersecurity service providers. The Act was fit-for-purpose given that most systems were still on-premise, and cloud use was not that widespread, while the tactics of malicious actors were not as sophisticated and advanced as they are today.

Singapore realised significant shifts in the operating landscape and specifically identified the adoption of Cloud Services which challenges the prevailing 'on-premise' model that the Act was originally predicated on. Furthermore, cyberthreat landscape has evolved, surfacing ICT supply chain complexities and associated risks. As a result, the CSA *noted* that regulating CII alone was no longer sufficient and the agency needed to look at the broader cyberspace, and other important information systems, extending the act's coverage to include important entities and foundational digital infrastructure. These legislative changes were enacted in 2024, when Singapore strengthened its legal and regulatory framework to address this growing threat and announced the significant amendments to the Cybersecurity Act.

The key characteristics of Singapore's evolving approach to critical infrastructure protection over the past five years – including amendments to the 2018 Cybersecurity Act – are as follows:

- 1. Singapore's legal framework primarily focuses on critical information systems used in the provision of essential services (CII) rather than a broader definition of Critical Infrastructure.** This reflects Singapore's emphasis on protecting digital systems, rather than physical infrastructure alone. In doing so, this approach focuses the attention on the systems which a CII owner uses to deliver essential services, rather than all other systems they may use for other business functions and operations. CII is defined as a computer or computer system necessary for the continuous delivery of an essential service, and the loss or compromise of the computer and computer system will have a debilitating effect on the availability of the essential service in Singapore; and the computer or computer system is located wholly or partly in Singapore. The Cybersecurity Act also defines '**essential service**' as any services essential to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.
- 2. The 11 CII sectors** include energy, water, banking and finance, healthcare, transport (which includes land, maritime, and aviation), infocomm, media, security and emergency services, and government. The 2024 amendments to the Cybersecurity Act expanded beyond the CII sectors to include **virtual CII computer systems, such as CII in a cloud environment.**
- 3. CII owners are designated by the Commissioner of Cybersecurity and the associated CII are then registered for regulatory obligations. Singapore adopts a three-tier governance model that reflects a balanced framework where responsibility is distributed among the Cyber Security Agency (CSA), sector regulators (Sector Leads), and CII owners.** The CSA plays a national-level role by setting policies, standards, and guidelines for CII protection. Sector leads regulators are responsible for implementing cybersecurity measures within their respective industries while balancing cybersecurity needs with operational requirements. And CII owners/operators bear direct responsibility for ensuring the security and resilience of their infrastructure.
- 4. Singapore's approach has also evolved to strengthen the regulatory oversight and enforcement capabilities.** The 2024 Amendments now allow the CSA as a lead agency to inspect CII if their owners fail to meet their obligations or if they provide inaccurate information; power to conduct on-site inspections of CII; and power to grant extensions for audit and risk assessment.
- 5. The national regulatory framework places the responsibility for cybersecurity on the owner of the CII or the provider of essential service.** This means that the entity delivering the essential service is held accountable for securing the systems necessary to deliver that service, regardless of whether the systems are on-premise or virtual. This approach draws on the expectations of fiduciary duties of the leaders of the CII owner and ensures that the entities directly responsible for delivering essential services are also responsible for protecting the underlying infrastructure, creating a clear chain of accountability. The text explicitly states that **cloud service providers are not regulated under the CII framework.** Instead, the **accountability for cybersecurity lies with the owner of the CII or the provider of essential service,** even if they rely on Cloud-based systems. This means that while Cloud service providers may host CII systems, they are not directly regulated under the

CII framework unless they are also the designated (and direct) providers of essential services. Thus the CII owners, not third-party CII vendors, remain accountable for their cybersecurity obligations for external systems provided by third party vendors. CII owners must establish **legally binding commitments** such as contracts to ensure their vendors' systems meet comparable cybersecurity standards.




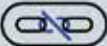

6. The 2024 Amendments also demonstrated a significant shift in Singapore's approach to regulate service providers (or providers of essential services). While before the CSA could only regulate CII if they were entirely or partially located in Singapore, the **2024 amendments expanded jurisdictions and allowed the CSA to regulate computer systems wholly located outside Singapore, provided two conditions are met:** (i) the owner of the computer systems is in Singapore; and (ii) such computer systems would have been designated as CIIs had they been located in Singapore. By extending its regulatory reach to systems located outside Singapore, **the amendments ensure that Singapore-based owners of critical systems are held accountable for cybersecurity, even if their infrastructure is hosted abroad.** This is particularly relevant for organisations that use Cloud services or offshore data centers to deliver essential services.
7. Singapore's evolving approach to CIP has extended to recognise **additional entities in the national regulatory framework.** There are three new types of entities in addition to CII owners, which are now subjected to the Cybersecurity Act:
 - a. Systems of Temporary Cybersecurity Concern ('STCC'), high-risk temporary systems that, if compromised, would seriously harm national interests. As STCC are systems that are important only for a limited time period from a cybersecurity perspective, the obligations placed on them also reflect this and many of the longer-term obligations placed on CII owners will not apply. STCC owners will not be required to carry out bi-annual cybersecurity audits and annual risk assessments. Owners of STCCs are also not required to participate in cybersecurity exercises.
 - b. Entities of Special Cybersecurity Interest ('ESCI'), organisations handling sensitive information impacting national interests.
 - c. Providers of 'Foundational Digital Infrastructure Service' ('FDI'), providers essential to the functioning of the digital economy, enabling the day-to-day needs of the citizens. The list of FDI providers has been specified in a new Third Schedule, which currently covers Cloud computing and data centre services. The list can be expanded to cover new types of digital infrastructure in the future.
8. **Expanded incident reporting obligations** highlight Singapore's priority to address supply chain vulnerabilities and third-party risks. Under the original Cybersecurity Act, CII owners were only required to report cybersecurity incidents affecting computers or systems that were interconnected with or communicated with the CII. This narrow scope meant that incidents affecting other systems under the CII owner's control, or systems managed by external suppliers, were not subject to mandatory reporting. The 2024 Amendments obliges **CII owners to report incidents affecting other computers or systems under the CII owner's control and computers under the control of external suppliers,** if those computers are interconnected with or communicate with the CII owner's CII.
9. **Incident reporting obligations have also been introduced for new entities:** STCCs must report cybersecurity incidents in respect of the STCC or any interconnected computer or computer system under the owner's control, or any computer or computer system under the control of a supplier that is interconnected with the STCC. The FDIs must report incidents where the incident results in a disruption to the delivery in Singapore of the major FDI service or has a significant impact on the major FDI service provider's business operations. The ESCIs must report incidents which result in a breach in the availability, confidentiality, or integrity of the entity's data or systems; or has a significant impact on the entity's business operations.

Key legislation and policies

The cornerstone of Singapore's legal framework for CIP consists of the *2018 Cybersecurity Act* and *2024 Amendments* to it.

UN GGE NORMS AND CBMS

UN GGE 2013 ([A/68/98](#)), UN GGE 2015 ([A/70/174](#)) and UN GGE 2021 ([A/76/135](#)) reports provide the following norms that were discussed in the Geneva Manual chapter 1 and 2:

F DO NOT DAMAGE CRITICAL INFRASTRUCTURE 	A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.
G PROTECT CRITICAL INFRASTRUCTURE 	States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199.
H RESPOND TO REQUESTS FOR ASSISTANCE 	States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.
I ENSURE SUPPLY CHAIN SECURITY 	States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.
J REPORT ICT VULNERABILITIES 	States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

Confidence-building measures (based on the UN GGE 2021 report):

- **Cooperative measures:**
 - Points of Contact, i.e. the identification of appropriate PoCs at the policy and technical levels to facilitate secure and direct communications between States to help prevent and address serious ICT incidents and de-escalate tensions in situations of crisis. Further information can be found in pp 76-78, [A/76/135](#), *UN GGE 2021 report*.
 - Dialogue and consultations through:
 - Bilateral, sub-regional, regional and multilateral consultations and engagement to advance understanding between States, encourage greater trust and contribute to closer cooperation between States in mitigating ICT incidents, while reducing the risks of misperception and escalation. Other stakeholders such as the private sector, academia, civil society and the technical community can contribute significantly to facilitating such consultations and engagement.
 - Regional bodies where inter-regional exchanges allow for mutual learning between regional organizations.

- CERTs/CSIRTs and other authorized bodies where States could encourage the sharing and dissemination of information and good practices on establishing and sustaining national CERTs/CSIRTs and on incident management. Further information can be found in pp 76-78, UN GGE 2021 report ([A/76/135](#)).
- **Transparency measures:**
 - Through the exchange of national views and practices on ICT security incidents and other related threats and by making ICT security advice, guidance, evidence base and data supporting decisions publicly available (on a voluntary basis).
 - By using bilateral, sub-regional, regional and multilateral fora and informal consultations to voluntarily share: information and good practices, lessons or white papers on existing and emerging ICT security-related threats and incidents; national strategies and standards for vulnerability analysis of ICT products; and national and regional approaches to risk management and conflict prevention, including national approaches to classifying ICT incidents in terms of the scale and seriousness of the incident.
 - By clarifying positions and voluntarily exchanging information on: national approaches to ICT security; data protection; the protection of ICT-enabled critical infrastructure; and ICT-security agency mission and functions, and ICT strategy at the national or organizational level, and the legal and oversight regimes under which they operate. Further information can be found in pp 82-86, UN GGE 2021 report ([A/76/135](#)).

Additionally some of the language from the CBMs sections (e.g. p 16) of the UN GGE 2015 report ([A/70/174](#)) were only partially included in the UN GGE 2021 report:

“To enhance trust and cooperation and reduce the risk of conflict, the Group recommends that States consider the following voluntary confidence-building measures: [...]

(d) The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include:

- (i) A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;
- (ii) The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure;
- (iii) The development on a bilateral, subregional, regional and multilateral basis of technical, legal and diplomatic mechanisms to address ICT-related requests;
- (iv) The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.”³⁴

³⁴ The highlighting has been added by the authors of this paper.

CONTRIBUTORS

The Geneva Manual on Responsible Behaviour in Cyberspace: Implementation of Norms by Relevant Non-State Stakeholders

March 2025

Published by DiploFoundation

Authors: Anastasiya Kazakova (DiploFoundation), Vladimir Radunović (DiploFoundation), Serge Droz (Swiss Federal Department of Foreign Affairs)

Illustrations: Vladimir Veljasevic (DiploFoundation)

Layout and design: Viktor Mijatović (DiploFoundation), Aleksandar Nedeljkov (DiploFoundation)

Contributors to the Geneva Dialogue in 2024 include both organisations and experts participating in their personal capacity:

- Private sector companies and organisations: ABB, Alibaba, AlixPartners, Bi.Zone (Sber Group), Cisco, CL2R Advisory, Cognizant, Ensign InfoSecurity, Ericsson, FireEye, Hitachi, Huawei, InfoGuard, Kaspersky, Mandiant, Microsoft, PNG Digital ICT Cluster, Proton, QI-ANXIN, Red Hat, SICPA, Siemens, Swisscom, Swiss Re, Swiss Risk Association, Tata Consultancy Services, Tech Mahindra, UBS, Wisekey, and Vu Security
- Academia and policy experts: Kamilia Amboudini, Winnona DeSombre (Atlantic Council), Kayle Giroud (Global Cyber Alliance), Bart Hogeveen (Australian Strategic Policy Institute), Imad Aad and Melanie Kolbe-Guyot (Center for Digital Trust (C4DT) – EPFL), Franziska Klopfer and Natalija Radoja (Geneva Centre for Security Sector Governance, DCAF), Lennart Maschmeyer (Center for Security Studies (CSS) at ETH Zurich), Jan Martin Lemnitzer (Copenhagen Business School), Katherine Getao (Cyber Hygiene, Cyber Diplomacy, and ICT Strategy and Governance Consultant, former CEO of ICT Authority in Kenya and the Kenyan representative to the UN GGE), Mischa Hansel (Berlin University of Economics and Law, HWR Berlin), Jen Ellis (NextJen Security), Benjamin Ang and Eugene EG Tan (S. Rajaratnam School of International Studies, RSIS), Alexandra Paulus (German Institute for International and Security Affairs, SWP), Christina Rupp (interface), Jeroen van der Ham (University of Twente and FIRST), Chao Wang (Wuhan University), Valentin Weber and Maria Pericas Riera (German Council on Foreign Relations, DGAP), Tom Wingfield (RAND)
- Technical community experts: Klée Aiken and Sherif Hashem (FIRST), Mirko Boehm (Linux Foundation), Pablo Corona Fraga (NYCEM Mexico), Pablo Hinojosa (APNIC), Koichiro Komiyama (JPCERT/CC), Steven Sim Kok Leong (OT-ISAC Executive Committee, Singapore), Maninder Singh Narang, Madison Q. Oliver (GitHub Security Labs), Takayuki Uchiyama, Igor Kumagin
- Civil society organisations and experts: Abdul-Hakeem Ajjola (African Union Cybersecurity Experts Group), Consumers International, CyberPeace Institute, CIPESA, DataSphere Initiative, Christopher James Sampson (Future Earth Systems), Global Forum on Cyber Expertise, Global Partners Digital, ICT4Peace

genevdialogue@diplomacy.edu
genevdialogue.ch

