ICC Working Paper

Protecting the cybersecurity of critical infrastructures and their supply chains

Executive summary

Protecting the cybersecurity of critical infrastructures and their supply chains is crucial for the simple reason that these systems power our daily lives—from electricity and water to healthcare and transportation. A cyber incident disrupting the functioning of these vital services can cause widespread chaos, endanger lives, and cripple economies. As cyber threats grow increasingly sophisticated and pervasive, ensuring the resilience and security of these critical systems is not just a technological necessity but a fundamental safeguard for the well-being and continuity of modern life.

This paper explores the complexities of protecting these systems stemming from multiple factors:

- Many of these services were not originally designed as essential services, leading to outdated technologies and structural vulnerabilities. The integration of digital components with physical systems amplifies risks due to the combined vulnerabilities of both realms, especially taking into account the rapid spread of new and emerging technologies.
- The increasing complexity and interdependence of supply chains expand the attack surface, making it essential to address third-party risks. Furthermore, the interdependence of these services with non-critical infrastructures complicates the establishment of clear boundaries and appropriate investment.
- Limited resources and budgets across both public and private sectors also hinder the implementation of robust security measures. Strong security practices, public-private collaboration, and international cooperation are crucial to safeguarding these vital systems, ensuring global economic stability, and maintaining trust in the digital economy.
- The distributed nature of digital capabilities requires global cooperation, yet there is a lack of international consensus and incentives. The definition of critical infrastructure varies globally, complicating international cooperation and coordination. Cross-border impacts and shared dependencies necessitate harmonised global efforts and aligned standards as well as sector-specific frameworks to mitigate risks effectively.

In providing a taxonomy and strategic recommendations to address these challenges the paper analyses the current state of cybersecurity for critical infrastructures and their supply chains, evaluates existing frameworks, policies, and technologies, assessing their strengths and weaknesses and identifying best practices as well as areas in need of enhancement.

The paper demonstrates how, in response to cyber threats, the private sector bolsters resilience and recovery by adopting comprehensive security measures, including embracing the principles of cybersecurity by design, maintaining robust asset inventories, developing incident response plans, implementing strong data backups, ensuring up-to-date systems with the latest security patches and zero-trust architectures, as well as a sound supply chain policy. It showcases best practices and existing industry standards that can be scaled up and more widely adopted.

At the same time, while business investment in prevention and defensive capabilities is essential, the private sector alone is unable to deter, prevent, or shield itself (and the communities it helps sustain) from the destructive effects of cyberattacks. **Cybersecurity is a shared responsibility between the private and public sectors, and both must work together to mitigate risks and curb cyber threats.** This is all the more important in the case of critical infrastructures where the roles and responsibilities of private and public sector actors are closely intertwined. **This paper calls for a close, continuous and joined-up relationship between critical infrastructure providers and governments to ensure effective responses to cyber threats.** It offers concrete recommendations for policymakers in domestic and international contexts alike, as well as suggestions for building effective public-private partnerships.

Table of contents

Introduction

While jurisdictions across the world have varying views of what specifically falls under this designation, *critical infrastructure* generally refers to the fundamental systems and assets, both physical and virtual, that are indispensable for the functioning of a society, its economy, and its essential services. Critical infrastructure is traditionally seen as a strategic element, facility, equipment, network or system, or part thereof, that cannot be replaced in order to provide an *essential service*. Such infrastructures are seen as crucial for the well-being and for preserving the public order and security of nations, thus their disruption could have significant consequences. They cannot be replicated or easily replaced in the short term and are therefore deemed to need special physical and digital protections. This may include sectors like energy, water, heating, transportation, finance, or communication. Most of these systems rely heavily on computer networks, control systems, and digital technologies, making them susceptible to cyber threats.

The concept of *essential services* is of particular relevance when designating an infrastructure 'critical,' and refers to the maintenance of vital societal functions, economic activities, public health and safety or the environment. This is all the more important as these services, their development or delivery becomes increasingly digital. In order to ensure the effectiveness of protection measures and legal certainty, this concept is often bound by a specific list of services deemed essential by policymakers.[1]

Ensuring trust in the digital economy requires the protection of the availability, integrity, confidentiality of these most essential infrastructures and services to ensure resilience. Digital and physical security go hand in hand to consolidate the operational resilience of organisations and the essential services they provide. Any failure in digital or physical security can lead to a serious incident in the disruption of service delivery and organisational reputation. Efforts should be focused on improving both the digital and physical security of services and increasing the resilience of critical assets against natural, accidental, or intentional events. Central to these efforts is the development of an appropriate and robust risk management framework, from identifying sources of risk to communicating incidents to stakeholders.

The purpose of this paper is to address cyber resilience measures, including collaboration mechanisms, private sector voluntary measures and, if needed, the balance between regulation and the sustainability of controls, for the protection of critical infrastructure and essential services, i.e. the ability of a critical entity to prevent, protect, respond, resist, mitigate, absorb, adapt and recover in the event of a cyber incident. While digital and physical protection measures need to be considered in a synchronised and increasingly coordinated manner, this paper focuses solely on the digital component. This is without prejudice to the need to consider other natural phenomena, human error, or misconfiguration outside the scope of this document when securing critical infrastructure or essential services.

While business investment in prevention and defensive capabilities is essential, the private sector alone is unable to deter, prevent, or properly shield itself (and the communities it helps sustain) from the destructive effects of cyberattacks.

1 US: www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
Europe: www.digital-strategy.ec.europa.eu/en/policies/nis2-directive
List of Essential Services: www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202302450

Cybersecurity is a shared responsibility between the private and public sectors, and both must work together to mitigate risks and curb cyber threats.

Governments are primarily responsible to protect their citizens, civil society and business from foreign and domestic, affiliated and unaffiliated threat actors with both political and criminal objectives, which also applies in cyberspace. Decisive action from governments to styme cyber threats and broad multistakeholder collaboration will help bolster economic confidence, prevent disruptions in global trade, and ensure a more secure cyber environment where businesses and communities can thrive. As set out in ICC Cybersecurity Issue Brief #2, enhancing multistakeholder cooperation to counter cybercrime and implementing rules for responsible state behaviour are essential to reduce cyberattacks, and thus increase security.[2]

This paper seeks to comprehensively address the multifaceted challenges surrounding the protection of critical infrastructure and essential services in the face of evolving cyber threats. By examining diverse perspectives on defining critical infrastructure and identifying the various actors, motivations, and impacts of cyber threats, we aim to underscore the urgency of a harmonised approach. Furthermore, by assessing the current state of protection efforts and highlighting areas for improvement, **this paper advocates for a coordinated approach involving private sector engagement, policy enhancements, international cooperation, and strengthened public-private partnerships**. Ultimately, our recommendations strive to bolster the resilience of critical infrastructure and essential services, as well as their supply chains, safeguarding them against emergent cyber risks in an increasingly interconnected global landscape.

2 ICC Cybersecurity Issue Brief #2: Implementing norms and rules for states and international cooperation

1. Varying approaches to defining critical infrastructure and essential services

Critical infrastructures form the backbone of the world's functionality and resilience. These essential systems and assets are the lifeblood of society. Disruptions to their security and proper functioning can have severe repercussions, affecting public safety, economic stability, and national security. We have seen the physical impact of critical infrastructure security around the world across varying sectors.

One example is Costa Rica's response to significant cyberattacks against public institutions in 2022, declaring a State of National Emergency in the public sector, highlighting the need for international cooperation.[3] This led to the creation of a General Emergency Plan, enhancing resources and administrative processes to address the issue. While these measures improved the response to attacks, the country recognised the need for a more comprehensive approach and is currently in the process of developing the National Cybersecurity Strategy 2023-2027, aiming to strengthen governance, adapt the legal framework, enhance infrastructure protection and national resilience, and foster cooperation in the digital environment. The strategy aligns with national strategic approaches and provides guidance for decision-making[4]. It also recommends prioritising the security of critical infrastructure by precisely defining national critical infrastructure, both in the public and private sectors, and outlining essential protection mechanisms. Additionally, the strategy emphasises the importance of strengthening risk management through the identification and prioritisation of critical assets, periodic cybersecurity risk assessments, and the allocation of resources to maximise the return on investment in terms of economic and social benefits.

Major incidents affecting critical infrastructure have had significant adverse impact across the globe and in multiple sectors over the past decades.

Some illustrative examples of major incidents affecting critical infrastructure include:

- In Europe, attacks on Estonian organisations including the Parliament, banks, ministries, newspapers, and others as early as 2007 were a wake-up call helping the country improve their cyber-defence tools.[5] In 2008, Georgia experienced major distributed denial of services attack on its critical infrastructure, including government services, the banking sector and various websites, with reportedly over 70% of Georgian websites affected.[6] A large number of similar threats were reported in the 2008-2014 period.[7] Most recently a number of attacks were reported in Ukraine (such as wiper ransomware) following the conflict with Russia.[8]
- In the US in 2013, hackers breached the Bowman Avenue Dam in New York and gained control of the floodgates. Oil rigs, ships, satellites, airliners, airport, and port systems were all thought to be vulnerable, and media reports suggest that breaches have occurred.[9]
- In May 2021, the Colonial pipeline ransomware attack forced all business operations to stop.[10]
- In Central and South America in January 2024, the Trigona attack on Claro operations caused over a week of disruption to services.[11]

While security of digital components in critical infrastructure serving essential services is key to safeguard resilience, **the combination of digital capabilities and physical components** as in Internet of Things (IoT) or Operational Technology (OT) **brings an explosion of potential new risks deriving from the joint effect of digital**

3 Executive Decree No. 43542-MP-MICITT 2022
4 www.micitt.go.cr/el-sector-informa/avanza-proceso-de-implementacion-de-la-estrategia-nacional-de-ciberseguridad
5 www.bbc.com/news/39655415
6 www.ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf
7 www.ccdcoe.org/uploads/2018/10/Ch08_CyberWarinPerspective_Weedon.pdf
8 www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology
9 www.industrialcybersecuritypulse.com/facilities/throwback-attack-how-the-modest-bowman-avenue-dam-became-the-target-of-iranian-hackers/
10 www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
11 www.commsrisk.com/ransomware-attack-hits-claro-across-latin-america/

vulnerabilities and the complexity of the physical world. One example of this was the case of Stuxnet,[12] by which a specialised malware was able to impair Iran's nuclear program through a digital attack to change physical parameters in Iranian nuclear SCADA systems.

These incidents highlight the potential destabilising effect of an attack on critical infrastructure and underscore the importance of strong security practice and collaboration among stakeholders to deter, protect and deal with cyber threats.

Furthermore, **in an increasingly interconnected world, the significance of critical infrastructure protection extends across borders to a global scale**. With shared dependencies and potential cross-border impacts, a breach in one region can impact another.

Cross-cutting cyber incidents that can be named range from the widespread Wannacry worm that affected all regions of the world,[13] to diverse vulnerabilities and attacks on the software and digital services supply chain, affecting organisations in different countries. One example is an incident that occurred in 2017, when the shipping giant Maersk, based in Copenhagen, Denmark became a victim of the NotPetya ransomware attack.[14] Maersk is one of the largest transportation companies in the world, responsible for one-fifth of the world's shipping. As a consequence of the attack, Maersk's freight operations in four different countries were affected, causing delays and disruptions that lasted weeks, while also costing the company over $200 million to remediate. Other recent examples are Log4shell,[15] SolarWinds,[16] and Ivanti.[17]

Harmonised efforts to set a baseline to protect critical infrastructure are crucial for fostering international collaboration, resilience against emerging threats, and ensuring the stability of the interconnected systems that underpin the modern world globally. By implementing globally aligned minimum protection measures, we can safeguard these fundamental assets against diverse threats, including national disasters, cyberattacks, and deliberate harm.

However, divergent global definitions of critical infrastructure and essential services, and contradictory requirements pose challenges for international cooperation and coordination to decrease cyber threats and to develop effective risk mitigating solutions. Misalignment can hinder effective communication and collaboration during cross-border crises. For an overview of various jurisdictions' take on critical infrastructure see **Annex I**.

> **The first step towards finding common agreement on terminology how to manage risks for critical infrastructure is convergence in using globally recognised, widely utilised international standards.**

For example, ISO Standards, the NIST Cyber Risk Framework, 3GPP in case of mobile infrastructure, and in case of the financial services sector the Cyber Risk Institute's 'Profile' can be utilised for complying with global financial regulations. Utilising such common standards helps ensure proper risk management with a high bar for security and privacy.

At the same time, critical infrastructure owners and operators are dependent on a web of third-party relationships to function. Therefore, supply chain and third-party risks are an extension of essential services. The rapid expansion of the digital economy in recent years, has exponentially increased the number of third parties in our ecosystems. As supply chains grow more complex, interdependent, and interconnected, risk exposure also grows. The attack surface increases, and the likelihood of an incident and the resulting cascading impacts becomes more challenging to predict, identify, and mitigate for critical infrastructure owners and operators.

Third parties are generally not designed to cope with such criticality in mind, either in terms of their technical and operational controls or their financial sustainability, which raises the dilemma of their feasibility to serve the purpose of such critical infrastructure and essential services.

The security of critical infrastructure is fundamental to our global economic security and the protection of trust in our shared digital economy. **Convergence on definitions, alignment of global standards and frameworks, and strong third-party risk management approaches can help raise the bar for security.**

12 www.spectrum.ieee.org/the-real-story-of-stuxnet
13 www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/
14 NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million (forbes.com).
15 www.ibm.com/topics/log4shell
16 www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T
17 www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

2. Challenges in protecting critical infrastructure

Given its paramount importance for the functioning of societies and economies, safeguarding critical infrastructure stands as principal challenge that requires a comprehensive understanding of the diverse landscape of cyber threats.

The digital threats faced by critical infrastructure and essential services are not fundamentally different than those facing any other digital capabilities, services, or processes.

The difficulty of adequate protection of critical infrastructures derives from several factors:

- Many of these essential services have not been deployed as such and have ended up taking on an essential relevance for society later. Thus, they were not conceived with a resilience criterion at the level of relevance they have ended up having. This could imply both a culture of protection below what is at present required and design problems that may affect how they can be protected now. An example is the very design of the Internet architecture where there are multiple structural risks that are difficult to patch without a root change (DNS structure, BGP decentralised protocols, insufficient levels of encryption and protection in protocols and services, insufficient roots of trust in encryption capabilities etc.)
- The interdependence of essential services and their corresponding critical infrastructures with other infrastructures or services that are not defined as such, makes it very difficult to determine the boundaries for the application of strict criteria, adequate investment, collaboration mechanisms, etc.
- The very distributed nature of digital capabilities makes it complex to be able to apply local policies without an adequate agreement between all countries, where there is a lack of global incentives or dissuasions to achieve a minimum of agreement on what should be protected, on the contrary, there is a risk of escalating aggressiveness between nations and blocs.
- The lack of knowledge and global vision of the nature of risks in both the public and private sectors makes it difficult to achieve standards beyond the need to protect all digital capabilities.
- The dispersion in complex digital supply chains also makes it difficult for public and private bodies to focus on simple criteria, making the problem extensive and dispersed.
- Some critical infrastructure components still rely on outdated and unsupported technologies, making them more vulnerable to cyber threats as security patches and updates may not be available.
- Many critical infrastructure organisations have limited resources and budgets allocated to cybersecurity, making it challenging to implement robust security measures and keep up with evolving threats.

In the following, we provide a structured analysis that encompasses the various dimensions of these threats, including the actors involved and their motivations, the various forms of threats, their impact, and complexities in responding to such threats. This taxonomy serves as a foundation for constructing effective cybersecurity strategies tailored to the intricate challenges posed by threats to critical infrastructure.

2.1 Actors and their motivation

Ranging from nation-states to cybercriminal organisations and insider threats, each actor is driven by distinct motivations that can extend beyond financial gains, encompassing geopolitical influence or event ideological pursuits.

State-nexus threat groups or advanced persistent threats

State-nexus threat groups are typically backed and directed by their military, intelligence, or other government departments. Unlike other groups mentioned in this context, they are generally well-funded and capable of conducting long-term plans to execute large-scale, advanced operations. Their main objectives could be revenue generation, espionage or destructive attacks, and they target both other countries and private organizations to obtain sensitive data, funding, or military strategies.[18] While the state sponsorship of some of them is still disputed, examples of such threats were claimed to include Stuxnet mentioned above, GhostNet reported to have compromised the devices of political, economic, and media targets in nearly 103 countries[19], Helix Kitten whose major targets included organisations in aerospace, energy, financial, government, hospitality, and telecommunications, mostly in the Middle East[20] or the more recently identified Flax Typhoon[21] claimed to gain and maintain long-term access to organisations' networks with minimal use of malware, relying on tools built into the operating system, along with some normally benign software to quietly remain in these networks.

Insider attacks

An insider attack refers to malicious acts carried out by an individual or a group of individuals who are associated with or employed by the target.[22] As actors are frequently engaged as either employees or independent contractors of critical infrastructures, they may be inclined to exploit deficiencies in critical infrastructures' monitoring systems rather than directly attacking the system from the outside. These insiders may either be direct employees of the impacted organisation or from a third party serving the essential service provider in its supply chain and frequently less subject to security controls and clearance. For example, in 2020, credentials of two Marriott employees were exploited to hack an application the company used as part of their guest services exposing the records of over 5 million guests.[23]

Hacker groups

Hacker groups frequently employ malware, phishing, or other hacking methods to attack critical infrastructures. They tend to infiltrate and disrupt the operations of critical infrastructures and engage in extortion tactics against governments or critical infrastructure providers.[24] It is worth mentioning that certain hacker groups, instead of directly engaging in cyberattacks, distribute ransomware to smaller groups or individuals, thus a part of a larger and complex ecosystem of very specialised cybercriminal organisations, more resilient to takedowns and prosecution. This trend has led to a significant rise in the number of criminals utilising ransomware and the overall magnitude of cybercrimes these days.[25] Examples include the Lazarus Group behind the WannaCry ransomware attack[26], REvil mostly known for the Kaseya attack and reportedly responsible for 37% of ransomware attacks in 2021[27] or Lapsus$ pursuing attacks against companies and government agencies with social engineering tactics.[28]

Hacktivists

Unlike the aforementioned attackers, hacktivists are usually motivated more by political or social views rather than financial interest. Most of the hacktivists engaged in cyberattacks do so with the intention of seeking alternative means to influence policy and bring about societal changes. It is important to note that their primary motivation is not personal gain. Nevertheless, this ideological aspect poses a potential challenge for providers of critical infrastructure services, as the attacks cannot be resolved through monetary solutions alone. For example, Anonymous has claimed responsibility for disabling prominent Russian government, news and corporate websites and leaking data.[29]

18 www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport
19 www.infosecinstitute.com/resources/threat-intelligence/ghostnet-part-i/#gref
20 www.wired.com/story/apt-34-iranian-hackers-critical-infrastructure-companies/
21 www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/
22 www.enisa.europa.eu/publications/enisa-threat-landscape-2020-insider-threat/@@download/fullReport
23 www.bbc.com/news/technology-54748843
24 www.techcrunch.com/2019/05/12/wannacry-two-years-on/#:~:text=Two%20years%20on%2C%20the%20threat,according%20to%20the%20latest%20data.https://techcrunch.com/2019/05/12/wannacry-two-years-on/#:~:text=Two%20years%20on%2C%20the%20threat,according%20to%20the%20latest%20data
25 www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystemhttps://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem
26 www.nccgroup.com/us/the-lazarus-group-north-korean-scourge-for-plus10-years/
27 www.newsroom.ibm.com/2022-02-23-IBM-Report-Manufacturing-Felt-Brunt-of-Cyberattacks-in-2021-as-Supply-Chain-Woes-Grew
28 www.theverge.com/22998479/lapsus-hacking-group-cyberattacks-news-updates
29 www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.htmlhttps://www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html

2.2 Threats and their impact

The types of threats posed to critical infrastructure, span from sophisticated malware and supply chain attacks to physical intrusions and denial-of-service assaults. While the methods used by malicious actors to disrupt the functioning of critical infrastructures are oftentimes similar to cyber threats in general, their potential to cause widespread and severe consequences is significantly more pronounced.

Cyber threats to critical infrastructure can lead to widespread disruption in essential services, affecting large populations. This can include power outages, transportation disruptions, water supply issues, and more, impacting public safety and the economy. They may pose direct threats to human safety. For example, disruptions to a transportation system could compromise the control of traffic signals or disturb railway operations, leading to accidents.

Given the highly interconnected and interdependent nature of critical infrastructure systems, a disruption in one sector can have cascading effects on others. For example, a power outage can impact healthcare, communication, and transportation systems. Furthermore, given the central role of critical infrastructures for the functioning of a country, disruptions to these systems can have significant national security implications.

It is important to emphasise that it is not only availability of these essential services which is important; in most cases, confidentiality and integrity are also affected and this is damaging society in similar or even more severe ways. For example, personal data leakage cannot be reverted once occurred and will harm people beyond the actual incident duration.

The most common threats on critical infrastructures and essential services include:[30]

Denial-of-service and distributed denial-of-service attacks

Cyber threats to critical infrastructure often include attempts to disrupt services through denial-of-service attacks (DoS), which are designed to flood a server with traffic, thereby making the website or online servers of critical infrastructure unavailable.[31] Additionally, a DoS attack may be conducted by using multiple computers to flood a targeted system, known as a distributed denial-of-service (DDoS) attack.[32] The focus may be on overwhelming communication networks, rendering them unable to coordinate and respond effectively.[33]

Targeted exploitation or disruption of industrial control systems

Cyber threats to critical infrastructure often involve the targeted exploitation or disruption of industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems, used to manage and automate critical processes in sectors like energy, water, and manufacturing. Unlike typical cyberattacks that primarily focus on data theft or system disruption, attacks on critical infrastructure may aim to manipulate physical processes. For example, a cyberattack on a power grid might attempt to disrupt the flow of electricity.

30 www.ericsson.com/en/blog/2023/10/deciphering-the-evolving-threat-landscape-security-in-a-5g-world

31 www.fortinet.com/resources/cyberglossary/dos-vs-ddos#:~:text=A%20denial%2Dof%2Dservice%20(,to%20flood%20a%20targeted%20resource.https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos#:~:text=A%20denial%2Dof%2Dservice%20(,to%20flood%20a%20targeted%20resource

32 Ibid.

33 The scale of DDoS attacks has increased over time. As per the findings of Google, a massive DDoS attack they blocked was 7.5 times larger than the largest attack they had previously blocked in 2022. Emil Kiner & Tim April, Google mitigated the largest DDoS attack to date, peaking above 398 million rps www.cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rpshttps://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps

Sophisticated malware

Cyber threats to critical infrastructure often involve sophisticated malware and advanced persistent threats. These threats are designed to remain undetected for extended periods, allowing attackers to gather intelligence, escalate privileges, and carry out coordinated attacks with significant impact.[34]

Exploitation of zero day vulnerabilities

Zero-day vulnerabilities are commonly gathered and exploited by the various types of malicious cyber actors. These vulnerabilities are especially serious since there is no way to know they are being exploited until some actual impact happens. The underground market for these vulnerabilities offers substantial illicit benefits to those who discover such vulnerabilities that surpass manyfold the rewards of legal bug bounty programs from the providers of the affected technologies.

Social engineering

Social engineering refers to the tactics used to exploit a human behaviour or error to gain access to internal systems. One of the most widely used tactics is phishing, where attackers adopt a false identity to send emails or text messages or make calls to unsuspecting victims. The goal is to trick them into submitting crucial information, such as bank account numbers or passwords, or unknowingly downloading malware.[35]

Physical access and hybrid attacks

Critical infrastructure often involves physical assets like power plants, dams, and transportation systems. Threat actors may attempt to gain physical access to these facilities, either directly or through insider threats, to compromise systems from within. They may employ hybrid attacks, combining various cyber techniques with physical actions. Multi-vector campaigns may involve cyber components alongside other forms of sabotage or disruption.

Triple extorsion

Triple extortion is a tactic used by ransomware attackers, where in addition to stealing sensitive data from organisations and threatening to release it publicly unless a payment is made, they also target organisations' customers and/or business partners and demanding ransoms from them too. This means that the attackers not only encrypt the victim's data and demand a ransom for its release, but also exfiltrate the data and threaten to release it publicly and launch a denial-of-service attack to further pressure the victim into paying the ransom.

Supply chain attacks

Attacking critical infrastructures through software supply chain is one of several possible threat vectors that attackers can exploit. Supply chain attacks are a growing and increasingly sophisticated form of cyber threat. They target the complex network of relationships between customer organisations and their suppliers, vendors, and third-party service providers vital to the supply chain.[36]

One supply chain attack taxonomy has been proposed by the European Union Agency for Cybersecurity (ENISA), see **Figure 1** containing four parts:

i. attack techniques used on the supplier,

ii. assets attacked in the supplier,

iii. attack techniques used on the customer,

iv. assets attacked in the customer.

A supply chain attack is a combination of at least two attacks: the first on a supplier that is then used to attack the target to gain access to its assets. The target can be the final customer or another supplier. Therefore, for an attack to be classified as a supply chain one, both the supplier and the customer have to be targets.[37]

34 www.securelist.com/apt-trends-report-q3-2023/110752

35 www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html

36 www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/

37 In the MOVEit supply chain attack, the attackers, CI0p, exploited a vulnerability in the MOVEit Transfer tool thereby gaining access to the data stored in the database. The incident affected more than 620 organisations. www.cyberint.com/blog/research/recent-supply-chain-attacks-examined/https://cyberint.com/blog/research/recent-supply-chain-attacks-examined/

Figure 1: Taxonomy for supply chain attacks

Supplier		Customer	
Attack techniques used to compromise the supply chain	**Supplier assets targeted by the supply chain attack**	**Attack techniques used to compromise the customer**	**Customer assets targeted by the supply chain attack**
Malware infection	Pre-existing software	Trusted relationship [T1199]	Data
Social engineering	Software libraries	Drive-by compromise [T1189]	Personal data
Brute-force attack	Code	Phishing [T1566]	Intellectual property
Exploiting software vulnerability	Configurations	Malware infection	Software
Exploiting configuration vulnerability	Data	Physical attack or modification	Processes
Open-source intelligence (OSINT)	Processes	Counterfeiting	Bandwidth
	Hardware		Financial
	People		People
	Supplier		

Source: ENISA, Threat Landscape for Supply Chain Attacks, 2021

2.3 Added complexities in responding to threats on critical infrastructure

In addition to the vast web of malicious actors and threats, one of the pivotal complexities in safeguarding these vital systems lies, in the nuanced interplay between the public and private sectors, where responsibilities for cybersecurity are often entwined.

Public-private collaboration and responsibilities

Whether critical infrastructure is managed by the public or the private sector, or a combination thereof, under the supervision of government authorities, it is imperative to establish clear delineation of duties and obligations between private sector and government authorities to facilitate cybersecurity. Specifically, the following should be clarified:

- **Vertical roles and responsibilities**: Government authorities function as supervisors, overseeing the overall direction and general target of cybersecurity requirements, as well as contingency actions during cyber incidents. On the other hand, businesses are the practitioners, bearing the lead responsibilities for maintaining the daily routine of cybersecurity. Failures to establish clear delineation of the roles and responsibilities may hinder the effectiveness of these public-private partnerships. For example, despite the importance of information sharing, the private sector might be reluctant to trust the authorities with their sensitive corporate information as this creates additional risks of unwanted data leaks and potential legal liabilities.[38] Given the complexities of this case, it is crucial for all stakeholders involved to collectively consider the option of adopting an alternative solution.
- **Horizontal roles and responsibilities**: More often, a cyber-incident may involve multiple government authorities, thereby complicating the roles and responsibilities regarding critical infrastructure. This often contributes to the different perspectives on the delineation of the authority between daily supervision

38 www.gost.isi.edu/cctws/delroso-ghosh.PDFhttps://gost.isi.edu/cctws/delroso-ghosh.PDF

and handling emergency of cyberattack.[39] In light of this, it is advisable that the delineation of roles and responsibilities among the central supervising authority, local supervising authority, and the authority of cybersecurity must be carefully defined in a variety of scenarios, including but not limited to daily maintenance, cyber incidents, and post-incident audits. Furthermore, the government should ensure that these delineations are clearly understood by both the authorities and the private entities involved.

Cross-border implications

Some critical infrastructure, such as finance networks or sub-sea cables often cross national boundaries and critical infrastructure supply chains exhibit even a greater degree of international linkages. Furthermore, cyber threats themselves know no boundaries. All this creates complications for businesses operating across several jurisdictions. As the operations of critical infrastructure may expand across national boundaries, it is important to recognise that the cybersecurity of critical infrastructure and supply chains will also be subject to the influence of global political conflicts, impacting business continuity of critical infrastructures and their supply chains.

For instance, in the current global landscape, some countries are imposing restrictions on the import and export of certain goods and technologies to safeguard their national security. Consequently, companies operating in multiple jurisdictions are facing growing compliance challenges and increased costs. This trend is particularly evident in cybersecurity, where governments are taking measures to protect their critical infrastructure from potential risks.[40]

Besides the geopolitical conflict leading to restrictions on critical components thereby obstructing the sourcing of components for the critical infrastructure, the uneven policymaking remains the broader and deeper issue at hand. As discussed above, though the general principle to identify a critical infrastructure is similar worldwide, there is no unified definition for critical infrastructure. In addition, the inconsistent contingency measures, reporting requirements and post-event improvement processes across the countries further complicate compliance for companies that provide domestic and cross-border critical infrastructure services and the suppliers of critical infrastructure supply chains.

For instance, in some jurisdictions, the competent authorities have designated particular critical infrastructure providers to be subjected to more stringent regulations. These regulations encompass the establishment of comprehensive cybersecurity maintenance plans and the mandatory reporting of any cyber incidents to the relevant authorities as soon as they become aware of such occurrences.[41] Conversely, certain jurisdictions, like Japan, do not explicitly identify critical infrastructure providers.[42] Instead, they develop their cybersecurity policies as non-binding guidelines, thereby not imposing an obligation on critical infrastructure providers to report cybersecurity incidents, unless said incidents pertain to personal data breaches or other heavily regulated industries. Notwithstanding, subsequent to the promulgation of the Act on the Promotion of National Security through Integrated Economic Measures, the competent authorities in Japan shall commence the identification of critical infrastructure providers and undertake additional supervision and regulatory measures.[43] In sum, a standardised framework is recommended for defining and implementing measures for the operation of the critical infrastructure and international cooperation.

39 In the case of an oil pipeline company, the competent authorities responsible for overseeing the company's daily routine should be the government sectors in charge of energy and transportation. However, when it comes to addressing a cyberattack, the competent authorities may be the sectors responsible for information infrastructure. In the case of a cybercriminal incident however, the pipeline company might only notify the sectors of energy and transportation for the hindrances of its daily operations, while disregarding the sectors of information infrastructure, which possess more competent capabilities to offer suggestions and prevent the further expansion of damages. www.cybersolarium.org/csc-2-0-reports/revising-public-private-collaboration-to-protect-u-s-critical-infrastructure/https://cybersolarium.org/csc-2-0-reports/revising-public-private-collaboration-to-protect-u-s-critical-infrastructure/

40 Both the US and China have implemented restrictions on the use of specific devices and components manufactured by the other within their respective jurisdictions in order to mitigate potential risks. With the increasing focus on cybersecurity, this approach is becoming increasingly common, resulting in heightened compliance costs for critical infrastructure operating across multiple jurisdictions. www.time.com/6295902/china-tech-war-u-s/

41 www.ec.europa.eu/commission/presscorner/detail/el/MEMO_16_2422)

42 www.dataguidance.com/opinion/japan-cybersecurityhttps://www.dataguidance.com/opinion/japan-cybersecurity

43 www.iclg.com/practice-areas/cybersecurity-laws-and-regulations/japanhttps://iclg.com/practice-areas/cybersecurity-laws-and-regulations/japan

Cost implications

As critical infrastructure delivers the services which are most fundamental to people's lives, companies often have to perform a balancing act between offering those vital services at a competitive price to consumers and ensuring that critical infrastructure is as resilient as possible. Governments should be cognisant of this fact and think about how to support companies to improve resilience.

As previously mentioned, critical infrastructure is vital to a country's operation it is often built, operated, and owned by the private sector. To safeguard the basic welfare of the public, many governments implement price regulations on the services that are essential to the public, including water, energy, and telecommunications, often in consideration of the domestic economic condition. Consequently, the imposition of price regulation may hinder the private sector's capacity to generate profits.

For instance, in Finland, the Electricity Market Act serves as the governing legislation for the energy industry. One crucial aspect that it addresses is the establishment of outage time limits, accompanied by corresponding penalties in the form of compensations to consumers. In the 2013 amendment, the Electricity Market Act introduced additional requirements for operators to meet resilience targets for weather hazards, which they must adhere to by the end of 2028 and are required to submit an investment plan to the energy authority every two years to demonstrate their progress. On the other hand, the regulation allowed these operators to raise distribution prices, up to a maximum increase of 30% in some instances. However, due to strong public and political reaction, the price increase was later capped at 15% per year, thereby creating cash-flow problems for some operators. This example highlights that despite the importance of improving the resilience of the critical infrastructure, balancing public expectations and operators' incentives and affordability is equally important.[44]

Given the private sector's profit-driven nature, it is advisable for government authorities to promote cybersecurity across the critical infrastructure providers through the implementation of tax deductions, loans with prime rates, subsidies, and other incentives.

44 www.oecd-ilibrary.org/sites/93ebe91e-en/index.html?itemId=/content/component/93ebe91e-en

3. Protecting critical infrastructure and supply chains – where are we now?

3.1 Protecting critical infrastructure and essential services

The mechanisms for applying digital protection to critical infrastructures (whether digital or not) and essential services are already well known and, apart from new risks that may arise with the arrival of new paradigms such as AI or quantum computing, the basic security processes can be identified in any of the standard cybersecurity frameworks that various organisations (ISO, NIST, ISF, etc.) have been developing over the past few decades. The real difficulty comes from the impossibility of protecting everything for a simple matter of efficiency or even effectiveness (complex ecosystems cannot be secured with simple processes as they require segmentation for focused protection).

Industry best practices

In response to cyber threats, the private sector bolsters resilience and recovery by adopting comprehensive security measures, including maintaining robust asset inventories, developing incident response plans, implementing strong data backups, ensuring up-to-date systems with the latest security patches and zero-trust architectures, as well as a sound supply chain policy. Cybersecurity training also comes into play as a crucial component, giving employees the necessary knowledge on best practices, aiming at building a strong security posture of systems and services from the inside out.

Generally, businesses recommend the following tools and good practices to prevent or tackle cybersecurity attacks:

- Maintaining an effective inventory of assets and robust perimeter surveillance with vulnerability management tools. This is especially important for critical infrastructure protection.
- Regularly backing up important data, stored in a properly protected system.
- Establishing security privilege policies to restrict unnecessary user access, while keeping systems up to date with the latest security patches. This is particularly relevant in the case of OT systems with access to non-replicated or safety-critical infrastructure.
- Utilising endpoint detection and response (EDR) systems, including multifactor authentication for publicly exposed assets.
- Implementing advanced cross-layer detection and response solutions on all platforms.
- Employing up-to-date antivirus signatures and configuring firewalls at the application level.
- Paying attention to vulnerabilities in backup and storage appliances, VPN software, and gateways and patching software to address vulnerabilities for both server and client applications.
- Applying zero trust principles across network architecture.
- Adding cyber-defence capabilities (based on SOC – Security Operation Centre) to processes, technologies, and operations, as well as the development of detailed incident response plans (IRP), with procedures for incident response strategies and providing dedicated incidence response teams (IRT).
- In the face of potential operational disruptions and financial burdens, essential service providers are increasingly turning to partnerships and cooperative initiatives as a cornerstone of their defence. Monitoring of cyberattacks trends, information sharing and collaboration with regional authorities and other essential services providers is key.
- In cases of cyberattacks, deploying forensic investigation to analyse the whole modus operandi employed by the attackers, assess the vulnerabilities that performed the initial access, and identify whether the cybercriminal accessed sensitive information or breached integrity allows future improvements.
- Conducting cybersecurity trainings to educate employees, performing regular security audits to test mechanisms and minimising external exposure to the internal networks.

- Consider that the supply chain is key not only to maintaining the efficiency and quality of service to customers, but also to ensuring that the potential compromise of one element of the chain does not affect other elements and the service as a whole. This has been the case in some of the most high-profile recent incidents (SolarWinds, Colonial, more recently the Ivanti VPN vulnerabilities, etc.).
- Consider on-demand support and the formation of coordinated defence teams that operate across national boundaries to provide rapid and effective responses during large-scale cyber incidents. These teams will play a pivotal role in mitigating the impact of significant cyber threats on critical infrastructure.[45]

So, which are the key aspects that should prevail in order to significantly improve the level of resiliency of essential services and critical infrastructure protection? To minimise the impact of potential disruptive situations, essential service providers need to build resilience and adopt best practices in risk management to protect critical infrastructures and end-to-end services.

Adopting the new Business Under Disruption way of working involves working in aspects such as:

- Identifying essential assets and services and defining downtime and recovery times.
- Understanding the interconnectedness of the business with other businesses, with particular attention to the supply chain.
- Using linked risk scenarios, updating risk map and concurrent event scenarios. It should cover activities such as identification (of assets), protection, prevention, detection, response, recovery, learning, evolution, and communication. Risk management will include the digital operational resilience strategy including, among others, performance indicators, deviation treatment, risk measurement parameters, test execution, incident reporting, audits, etc. to achieve the specific ICT objectives, as well as, among others, the risk analysis methodology for confidentiality, integrity, availability, and authenticity of information.
- Performing tests on systems in production and determining the level of awareness.

Policy and regulatory approaches to cybersecurity of critical infrastructures

As said above, any of the existing cybersecurity frameworks is sufficient in itself to increase the resiliency of such services and infrastructures (digital-wise). Examples are the Cybersecurity Framework (CSF) from NIST or the recently updated ISO27001:2022 that brings the more structured ISMS (information security management system) approach on board.

Different regulatory schemes intend to contribute by setting requirements (instead of standards) such as DORA for the financial sector or NIS2 for digital providers and the Cybersecurity Resiliency Act that encompass, not just critical infrastructures but digital products. Best practices are yet to take hold once the DORA regulation is in place and the Regulatory Technical Standard (RTS) will be published in 2024. However, work can begin on meeting design requirements to ensure a solid foundation for the digital operational resilience of critical enterprises and entities.

However, the dynamics of the markets for different services place severe constraints on how much a key service provider can demand and evaluate security requirements. While certifications to cybersecurity frameworks serve this purpose, they are still limited in a scenario of decreasing business margins, where all parties in the services are looking for reduced costs and efficiencies in order to cut corners on controls (security controls therein).

Also, at national level different regulations exist to bring down to earth more generic frameworks and to ease further compliance check by regulatory bodies.

These include for example the ENS in Spain for the public sector, TSA in UK for communication service providers,. In China, the Ministry of Transport released CII Security Protection Management Measures for the transportation sector, which requires CII operators in transportation sector to comply with a series of compliance obligations. In Australia the Security of Critical Infrastructure (SOCI) Act (2018)[46] defines critical infrastructure sectors and sets out their obligations. As part of a major wide-ranging national Cyber Security Strategy (2023-2030),[47] the government is in the process of drafting a number of key amendments to the SOCI

45 www.digital-strategy.ec.europa.eu/en/policies/cyber-solidarity
46 www.legislation.gov.au/C2018A00029/latest/text
47 www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

Act, which will, among other things, include data storage systems in the scope of business critical data (of a critical infrastructure asset), improve national responses to significant incidents, simplifying government/industry information sharing in crisis situations, and consolidating telecommunications security requirements in the one Act. These amendments (and the strategy more broadly) seek to ensure that the right entities and assets are being protected, ensure compliance with cyber security obligations, and provide the needed help to critical infrastructure to manage the consequences of cyber incidents.

Appropriate mapping across these frameworks is required, as in many cases essential service providers have to deal with different regulatory demands across geographies and sectors of activity (e.g. a financial arm of an Internet service provider may have to comply with both telecoms and financial regulations, and a number of others depending on the countries and customers it serves).

3.2 Securing the supply chain of critical infrastructures

The current state of Cyber Supply Chain Risk Management (C-SCRM) across critical infrastructure sectors globally is difficult to generalise. On the one hand, it is fair to say that a significant portion of critical infrastructure in some markets is owned and operated by the private sector. In the US, official estimates place private ownership of critical infrastructure at 85%.[48] In the EU, it is 80%.[49] In the UK, approximately 50% of critical infrastructure is owned and operated privately[50], while in many other markets, such as in China, the Middle East and others, state ownership of critical infrastructures is the prevalent model.

On the other hand, however, the various private sector and state-owned entities that constitute the global community of critical infrastructure owners and operators are as diverse as they are numerous. These entities span the spectrum from large, multinational corporations to small, independent producers, service providers, independent contractors, and sub-contractors.

Aside the difference in ownership models across countries, the definition and hence the scope of what is deemed a critical infrastructure in a given jurisdiction varies across countries, from none to comprehensive definitions and frameworks as shown in **Annex I.** Differences in key definitions among others may lead to international policy challenges, when attempting to develop international best practices and rules that aim to strengthen cybersecurity and resilience of critical infrastructures at regional or global level.

The World Economic Forum's Global Cybersecurity Outlook 2024[51] identified among others a growing cyber-resilience gap between large, small- and medium-sized enterprises highlighting an additional challenge when considering the security and resilience of supply chains of critical infrastructures.

The situation is further aggravated by an expanded threat surface, by connecting through IoT operational technologies controlling the systems of energy, water, sewage, and other critical infrastructures. This is since the practice of "air gapping," or physically segregating digital networks has given way to the demands of broader interconnectivity through IoT technology and legacy systems integration with more modern software, supply chain breaches have become an attack vector favoured by malicious actors.

It follows, then, that all these entities operating critical infrastructures have varying modes of ownership, face different regulatory frameworks, possess different degrees of resources, expertise, and capacity to properly secure operations and their supply chains.

What is cybersecurity of supply chain about?

As in security more broadly, cybersecurity is also a risk-management activity as there is no such thing as 100% security. In principle, risk management procedures consist of four core tasks: risk identification, assessment and measurement of risks, treatment, and monitoring. One high-level descriptive example of a risk management process is provided by the Australian Government.[52]

48 www.gao.gov/products/gao-09-654r
49 www.gisreportsonline.com/r/europe-critical-infrastructure/
50 www.nic.org.uk/themes/design-funding/
51 www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
52 www.austrac.gov.au/business/core-guidance/amlctf-programs/implement-risk-management-process

Exploiting vulnerabilities in existing software supply chains rather than targeting end-users has enabled these actors to magnify their impact compromising multiple accounts simultaneously and surreptitiously breaching accounts that may be more difficult to infiltrate directly.

While supply chain cyber infiltrations are not a completely new phenomenon, with multiple known supply chain breaches occurring as far back as 2013,[53] the discovery of the breach of Solar Winds' Orion IT monitoring and management platform in December 2021 marks a watershed event in the growth of this threat vector. Statista, the online statistics and survey platform, reports that the number of software packages worldwide affected in known supply chain attacks increased from 700 in 2019 to more than 185,000 in 2022[54] and there is no end in sight. Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.[55] Total economic loss from supply chain attacks, albeit a fraction of aggregate cost of cyberattacks[56] is expected to grow exponentially. Cybersecurity Ventures, a leading cybersecurity researcher, forecasts that economic loss to global business from supply chain attacks will grow by 15% year-over-year for the next years. Thus, the 2023 estimated cost of $45 billion is expected to rise to $138 billion by 2031.

The good news is that government and industry have begun to take notice and are taking action. There is widespread recognition that to achieve more effective supply chain security practitioners must address the problem comprehensively. For example, mitigating software supply chain risk requires that sound security practices be incorporated into the inhouse coding process at the beginning of the product development cycle securing third part commercial software as well as open-source software. Thus, in well-resourced organisations with mature security programmes, developers have adopted practices, such as consistent code reviews, disciplined internal vulnerability management and aggressive patching protocols, especially concerning third-party dependencies.[57]

Industry best practices

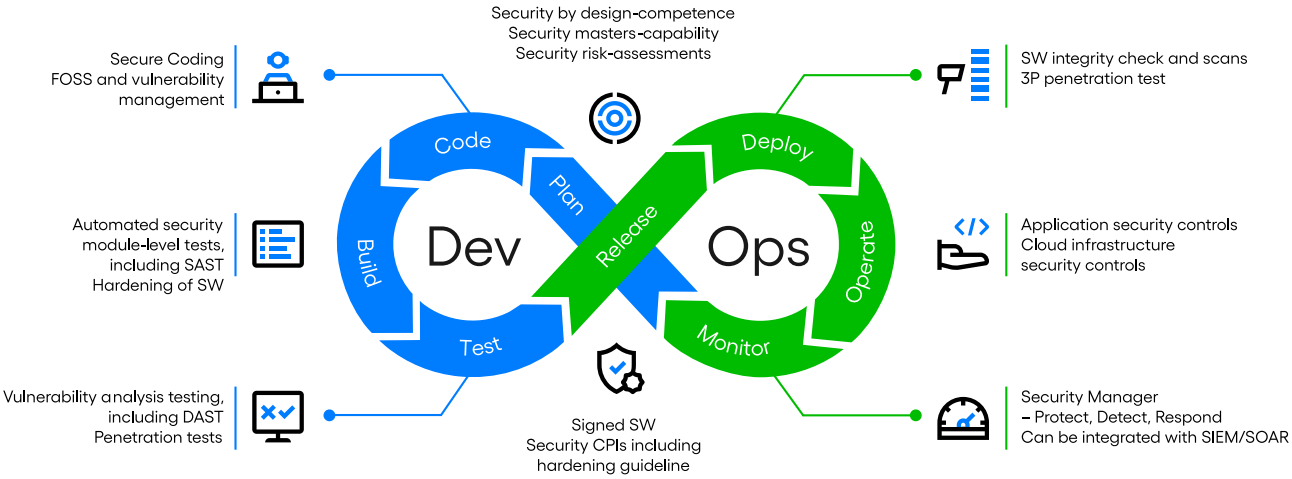
Regarding the protection of supply chain, the use of best practices[58] like the ones below could be considered:[59]

1. **Focus on a set of priority security requirements** based on an assessment of risk, a short list instead of over-loading the supplier, and ensure monitoring, oversight, and compliance. In addition, take into account the industry references and recommendations when they are available such as IEC 62443 in industrial cybersecurity.
2. **Reduce the impact of third-party incidents via discrete actions** like diversifying the supply chain, applying zero trust policies[60,] developing incident response plans, conducting tests, and demanding early reporting of incidents by suppliers.
3. **Actively partner with suppliers** to help them improve their security programmes, offering service mechanisms and trainings to protect against or respond to incidents as they occur. Third-party incidents will happen, so preparing to manage the impact on the enterprise must be a core priority.
4. **Consider leveraging emerging technologies** such as blockchain for information sharing and asset management to minimise the consequences of third-party cyber incidents, as well as artificial intelligence and advanced analytics to scale incident detection and response capabilities.
5. **Add incentives and enforcements to contracts**, setting requirements for suppliers based on international standards (e.g. ISO 27001 Information Security, ISO 27701 Privacy, ISO 22301 Security and resilience).
6. **Establish processes to increase business leaders' involvement** in managing third-party cyber risks. Doing so needs to be a priority at the most senior levels.

53 www.reversinglabs.com/blog/a-partial-history-of-software-supply-chain-attacks
54 www.statista.com/statistics/1375128/supply-chain-attacks-software-packages-affected-global/
55 www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022
56 www.weforum.org/publications/global-cybersecurity-outlook-2024/
57 www.go.snyk.io/2023-supply-chain-attacks-report-dwn-typ.html?aliId=eyJpIjoidFd0SVpwb0R6M2VNeUMrMyIsInQiOiJGRUE3VFdwTDB4Tk95TzkzTERadzRRPT0ifQ%253D%253D
58 www.cybertechaccord.org/best-practice-alignment-for-supply-chain-security-across-standards-and-regulatory-frameworks/
59 www.email.rsaconference.com/p/7K6E-7LN/nur-48-2023esaf-formhttps://email.rsaconference.com/p/7K6E-7LN/nur-48-2023esaf-form
60 www.cybertechaccord.org/zero-trust-once-again/

In the context of ICT supply chain risk management, for example, a supply chain risk management process[61] could cover internal software development, consumption of upstream third-party software, including open-source software, secure coding practices, vulnerability scanning, vulnerability testing, penetration tests, and operations. It is important to recognise that software supply chain security is just one element of supply chain security, but from a cybersecurity perspective, a key one to consider. Due to technological evolution in how software is developed and delivered, such as continuous integration and continuous delivery (CI/CD) workflow, DevSecOps[62] has evolved to address the need to build in security continuously across the software development life cycle. Another important development in the app-driven world is the application programming interface (API). Simply put, an API is a type of software that acts as an interface or connection point, enabling two different applications or functions to communicate with each other. From banks, retail, and transportation to communication networks, IoT, autonomous vehicles and smart cities, APIs are a critical part of modern mobile, software as a service (SaaS) and web applications and can be found in customer-facing, partner-facing and internal applications. Taking these and other technological developments, a secure software supply chain based on SRM is visualised in **Figure 2.**

Figure 2: Securing the software supply chain based on the Ericsson Security Reliability Model



Source: Ericsson, Security Reliability Model, 2021

Open-source software security

Many ICT vendors and communication service providers leverage open-source software (OSS) for their software projects and products with the purpose to enable communications service providers to build open, interoperable networks at a lower cost. Examples of industry collaborations promoting the use of open-source code are the Open Network Automation Platform (ONAP) and O-RAN Software Community (OSC) hosted by the Linux Foundation, and Openstack hosted by the OpenInfra Foundation. OSS has inherent benefits that can provide secure code, but also has inherent security risks that require a higher level of due diligence. It is the responsibility of the software product vendor to ensure proper safeguards are in place for secure use of shipped product with OSS and proprietary software components.

The Open Source Security Foundation (OpenSSF) is another organisation that is promoting standards for assurance of open source across the industry.[63]

Use of open-source software requires a higher level of due diligence which organisations can implement by applying industry best practices for supply chain management, secure software development, and secure software maintenance. There are government and industry organisations available to help, including DARPA AIxCC[64], the US Department of Commerce's National Institute of Standards (NIST), The Linux Foundation, and

61 www.ericsson.com/en/security/ericssons-security-reliability-model
62 www.synopsys.com/glossary/what-is-devsecops.html
63 www.openssf.org/
64 www.aicyberchallenge.com/

OWASP. The Linux Foundation Core Infrastructure Initiative has a Best Practices Badge for open-source projects to self-attest. OWASP has made available many automated vulnerability detection tools that are available for free to open-source projects.

According to CISA[65], in order to secure open-source software, it is important to understand the relevant attacks and vulnerabilities. CISA is broadly concerned **about two distinct classes of open-source software vulnerabilities and attacks**:

1. The cascading effects of vulnerabilities in widely used open-source software. As evidenced by the Log4Shell vulnerability, the ubiquity of open-source software can cause vulnerabilities to have particularly widespread consequences. Given the prevalence of open-source software across government and critical infrastructure including the widely use of open-source software in closed-source software, the widespread and distributed nature of open-source software can magnify the impact of open-source software vulnerabilities.
2. Supply-chain attacks on open-source repositories leading to compromise of downstream software. The second category of risks is the malicious compromise of open-source software components, leading to downstream compromises. Examples include an attacker compromising a developer's account and committing malicious code, or a developer intentionally inserting a backdoor into their package. Real-world examples include embedding crypto miners in open-source packages, modifying source code with protestware that deletes a user's files, and employing typosquatting attacks that take advantage of developer errors.

Policy and regulatory approaches to cybersecurity of supply chains

The globalisation of the enterprise supply chain poses new challenges to ensure effective risk management in line with national security interests, which may call for tailor-made requirements.

Indeed, governments around the world are using the power of regulation and legislation to encourage, and in some cases, mandate secure software development practices. In the US, the Biden Administration issued the Executive Order on Improving the Nation's Cybersecurity (EO 14028) in May 2021, on the heels of the discovery of the SolarWinds breach. Among other things, the EO mandated that commercial software utilised by the federal government must adhere to certain guidelines. These guidelines, developed by the National Institute of Standards and Technology (NIST) and released in two separate publications in February 2022, the NIST Special Publication (SP) 800-218: Recommendations for Mitigating the Risk of Software Vulnerabilities and the NIST Software Supply Chain Security Guidance require federal agencies and private sector providers contracting with the federal government to employ such measures as encryption, continuous monitoring, multi-factor authentication, vulnerability management, Software Bills of Materials (SBOMs) and numerous other requirements. While not mandatory for private sector providers outside of the government contracting space yet, they use of these guidelines establishes a standard of supply chain security that is widely recognised and encouraged, elements of which may become mandatory in subsequent legislation and/or regulation.

In September 2022, the European Commission proposed the Cyber Resilience Act (CRA) to improve cybersecurity and cyber resilience in the EU. The CRA aims to establish common security standards for all products with digital elements in the EU. The CRA will require manufacturers of products with digital elements to implement appropriate cybersecurity measures across the lifecycle of the product. This will include conformity with "essential cybersecurity requirements" during the design and development stage with initial cybersecurity assessments and ongoing vulnerability management and updates as well as incident reporting throughout the product lifecycle. Common agreement on the final text of the CRA was reached in December 2023 and a final approval from the European Parliament and the European Commission is expected in 2024. In addition, Europe's recently approved Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA), applicable from January 2025, will test the waters further on supply chain protection. It includes provisions on contracts, security standards, management of risks, rights of access, inspection and audit on suppliers, risk and resilience training and awareness-raising for staff and governance structures for security management, among others.

65 www.cisa.gov/sites/default/files/2024-02/CISA-Open-Source-Software-Security-Roadmap-508c.pdf

GSMA and NIST have developed IoT security guidelines for manufacturers and their supporting third parties as they conceive, design, develop, test, sell, and support IoT devices across their spectrum of customers. According to GSMA, for the IoT to continue to evolve effectively, following security challenges must be addressed:

- **Availability**: ensuring constant connectivity between Endpoints and their respective services
- **Identity**: authenticating Endpoints, services, and the customer or end-user operating the Endpoint
- **Privacy**: reducing the potential for harm to individual end-users
- **Security**: ensuring that system integrity can be verified, tracked, and monitored

IoT security mitigations need to be tailored for customers, applications and/or environments. Tailoring can be for business sectors or vertical industries and can add requirements, edit specific requirements narrowing or expanding how they are applied or, in rare instances, delete requirements.

In October 2022, the UK National Cyber Security Centre (NCSC) released guidance for medium and large organisations to "gain assurance about the cybersecurity of their organisation's supply chain.[66] The guidance describes how organisations are exposed to vulnerabilities and cyberattacks through their supply chain and defines expected outcomes and key steps to help organisations assess the security of their supply chain. The guidelines are voluntary and there is no mandatory supply chain security legislation presently in the UK. At the present time, the UK is seeking to "find an appropriate legislative vehicle" by which to update the EU's Network and Infrastructure Systems (NIS) Directive of 2018, which it hopes to accomplish in 2024. The proposed amendments include many of the same supply chain security measures discussed in the US and EU legislation/regulation. In addition, the UK's Product Security and Telecommunications Infrastructure Act 2022 (PSTIA), replicates many of the provisions of the CRA with respect to digital products, including transparency on minimum periods for security support and vulnerability reporting, as well as banning default passwords. These provisions will become enforceable in April 2024.

In China, the Cybersecurity Review Measures (CRM) issued by the Cybersecurity Administration of China (CAC) in December 2021, established a cybersecurity review mechanism for CII's procurement of network products and services, which affect or may affect national security. Additionally, the Ministry of Industry and Information Technology (MIIT) and the CAC released the Administrative Provisions on Security Vulnerabilities of Cyber Products. The provisions require cyber product providers to take measures to manage security vulnerabilities of cyber products and report them to the Cyber Security Threat and Vulnerability Information Sharing Platform.[67]

There are also initiatives underway in other markets, such as the guidance by the Canadian Centre for Cyber Security on protecting organisations from software supply chain threats[68] or by the New Zealand National Cyber Security Centre on supply chain cyber security[69]. Nonetheless, much remains to be done.

The aim should be to achieve harmonised requirements across markets based on business best practices and international standards. Many past efforts to harmonise requirements and assessments have failed to reach agreement and have unfortunately increased the complexity of compliance, thereby increasing risk. As a result, it is proving difficult and costly for prime contractors for specific services to understand and manage the risks of multiple subcontractors.

International cooperation on incident reporting obligations for critical infrastructure operators is another welcomed area for cooperation where international alignment can decrease complexity and administrative burdens while at the same time ensure that relevant and timely information is available to increase situational awareness and over-time expanded cumulative knowledge. To further this development the steps taken between the US and EU to streamline incident reporting obligations should be further encouraged and also over time geographically broadened in relevant international forums.[70]

66 www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security
67 www.reuters.com/technology/china-conduct-cybersecurity-review-chipmaker-microns-products-2023-03-31
68 www.cyber.gc.ca/en/guidance/protecting-your-organization-software-supply-chain-threats-itsm10071
69 www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf
70 www.digital-strategy.ec.europa.eu/en/library/comparative-assessment-dhs-harmonization-cyber-incident-reporting-federal-government-report-and

Additionally, to sustain resilience, security, trust and competitiveness of networks and supply chains, diversification is key. National security decisions restricting the critical or sensitive components from specific vendors need to be based on objective criteria, proportionate, and effectively implemented. Exclusions of suppliers may have high impact on private critical infrastructure operators' costs but also impact national security, resilience, and market development. Hence, such decisions must also take into account that private operators of critical infrastructures are not accountable for national security nor necessarily considering national security risks in their business decisions.

A cooperative and coordinated approach among all stakeholders is the best means by which governments will raise the baseline cybersecurity standards, avoiding over reporting, while generating an efficient common trust-based practice, particularly in the supply chain. A holistic approach, enhancing multistakeholder cooperation to counter cybercrime and implementing rules for responsible state behaviour in cyberspace are essential to reduce cyberattacks, and thus increase security.

4. Towards better protection of critical infrastructures and increased supply chain security

The protection of the cybersecurity of essential services and critical infrastructure and their supply chains requires a balanced, well-targeted, and proportionate approach for all service providers of critical infrastructure and essential services, paired with an appropriate national and international regulatory framework with sufficient public capacity to enforce and incentivise appropriate behaviour.

As perfect cybersecurity is an elusive goal, residual risks need to be mitigated by measures aimed to decrease potential threats. These measures involve

i. disrupting cyber threat actors,

i. prosecuting cybercrimes more effectively, and

ii. fostering urgent, large-scale, and effective implementation of the widely agreed existing norms and rules for state behaviour in cyberspace by setting shared goals for action.

Well-designed public-private partnerships are also necessary for normative development and cross-sector investment to support the continued evolution of required level of protection and hence resilience of essential services and their supply chains.

The fundamental cybersecurity challenge to protect essential services, critical infrastructures, and their supply chains can be generally summarised into three points:

1. **Need for transnational agreements** for the establishment of baseline cybersecurity outcomes and objectives. Fragmentation at this level is not an effective cybersecurity approach, but rather creates complexity, inefficiencies and increased costs ultimately negatively impacting all stakeholders. Common approaches can be facilitated by:

    a. Alignment across supply chains on the development and use of technical security standards.

    b. Alignment on and implementation of risk-based security risk management frameworks for the suppliers and the operators of critical infrastructure and essential services.

    c. Clarity on the roles and responsibilities for cybersecurity across the value chain. Suppliers are accountable and responsible for their products and solutions, and operators of critical infrastructure and essential services are responsible for the security of critical infrastructure and services. Nation states are responsible to disrupt cyber threat actors and decrease cyber threats that critical infrastructure and essential service providers and suppliers are exposed to.

2. **Need to decrease cyber threats**, including cybercrime originating from criminal groups and threats by states or state-sponsored cyber actors.
3. **Identification of incentives and deterrents for cybersecurity investment** that isolate the resilience cores of essential services and critical infrastructure, likely changing the way such services and infrastructures are designed, deployed, and operated. Along the same lines, it would also be how the objectives of economic profitability and competition between service providers are balanced with the appropriate levels of public investment in support of the social relevance of essential services and critical infrastructures, beyond reinforcing with regulation the strict requirement of resilience of the same.

Neither of these three points can be solved by simple or immediate measures.

Recommendations for private sector actors

As noted in the 'industry best practices' sections above, businesses already work to apply the basic security controls helping to prevent the attacks and mitigate the risks. These efforts should be adopted and implemented at a large scale across regions and sectors. As a reminder, the common good practices are:

- Implement a cybersecurity risk management framework for assets and their supply chain;
- Ensure to follow suppliers' configuration and hardening recommendations when deploying assets into operational environment;
- Maintain an effective inventory of assets and robust perimeter surveillance with vulnerability management tools;
- Regularly back up important data, stored in a properly protected system and perform restoration tests;
- Pay attention to vulnerabilities in backup and storage appliances, VPN software, and gateways and patching software to address vulnerabilities for both server and client applications;
- Establish a zero trust approach, following the principle "never trust, always verify" and across network architecture;
- Utilise multifactor authentication;
- Utilise endpoint detection and response (EDR) systems, while being mindful that automated response can lead to service disruptions unless well tested in the specific context, including in EDR configuration changes and life cycle management.
- Implement advanced and automated cross-layer detection and response solutions on all platforms while minimising negative impacts on the expected quality of service;
- Employ up-to-date antivirus signatures and configure firewalls at the application level;
- Add cyber-defence capabilities to processes, technologies and operations;
- Develop detailed incident response plans (IRP), with procedures for incident response strategies and set up a dedicated incidence response team (IRT);
- Conduct crisis drills often to understand the organisation's level of preparedness;
- Conduct cybersecurity trainings to educate employees, perform regular security audits to test mechanisms and minimise external exposure of the internal networks; and
- Consider that the supply chain is key not only to maintaining the efficiency and quality of service to customers, but also to ensuring that the potential compromise of one element of the chain does not affect other elements and the service as a whole.

Recommendations for policymakers

- If not already in place, set up an independent cybersecurity agency with specialised staff and budget and specified goals and means including regularly coordinating cyber exercises.
- Adopt a holistic[71] public cybersecurity approach that i) considers the entire lifecycle of products and services on which operators rely, ii) gathers all relevant stakeholders and iii) is coordinated across the entire government and at the international level.
- Given the increasing complexity of communication networks' supply chain and lifecycle, no single stakeholder can be held entirely responsible for enhancing overall digital security. Thus, when governments design policies to enhance the digital security of communication networks, they need to consider the following four categories of stakeholders, which have a specific role in digital security risk management:

71 www.oecd-ilibrary.org/science-and-technology/enhancing-the-security-of-communication-infrastructure_bb608fe5-en

- Communication network operators;
- Users, including industrial users such as operators of other critical activities;
- Suppliers of products and services, including hardware equipment and software, system integration, managed services, and cloud services; and
- Standard development organisations (SDOs).

- There is often a patchwork of legislative instruments regulating cybersecurity obligations affecting the same actors and different agencies in charge. A holistic approach also includes coordination and alignment in demands across different governmental agencies, such as the government department in charge of communication policy, the communication regulator, the digital security regulator, the competition authority, the department in charge of economic development, and others. A clear definition of responsibility and/or mandates between the different bodies is also essential.
- Develop a national security plan for critical infrastructure and essential services in partnership with the private and public sectors.
- Ensure transparency on designation of critical infrastructure and essential services, working with industry to determine how critical infrastructure should be identified, including supply chain risk mitigation and covered suppliers.
- Improve policies on the protection of supply chains, including the implementation of international standards, and mutual recognition of regional standards.
- Create information sharing mechanisms, both voluntary and mandated, and ensure that there is a two-way flow of information.
- Ensure that businesses know exactly which agencies are involved in not only the regulation of critical infrastructure, but also in assisting in the event of an attack.
- Build a culture of cybersecurity and ensure the development of cybersecurity talent.
- Invest in capacity building (including human capital), raising awareness and effectively fighting against cybercrime.

Recommendations on effective international collaboration

A holistic national policy framework is more likely to be effective if coordinated at the international level, as supply chains for communication networks are global and interconnected. No country alone would be able to build the entire supply chain of products and services critical to communication networks from scratch. Therefore, governments should:

- Strive to harmonise regulatory approaches on an international and cross-sector basis.
- Enumerate critical infrastructure sectors – on their own and in diplomatic forums – to include traditional sectors such as water, food or energy, as well as the IT sector and in particular cloud services which underscore the maintenance and delivery of essential services.
- Recognise at the United Nations a new norm prohibiting state-sponsored cyberattacks targeting the ICT supply chain.
- Routinely issue public attribution statements following cyber incidents conducted by state actors that violate international norms or rules, noting more precisely which expectations were violated.
- Establish robust deterrent consequences for state-sponsored cyberattacks targeting critical infrastructure which reflect the costs associated with repair and any potential harms threatened by the attack.

Recommendations on effective public-private partnerships

- Make cybersecurity investment an integral part of the government's national development plan. Rapid digitalisation is testing the resilience of private and public services and infrastructures, which in turn means that cybersecurity must be integrated into a country's modernisation policy. As a best practice, some countries even set aside between 10% and 20% of the public support budget for each digital transformation project for cybersecurity, to promote cybersecurity by design. Collaborative promotion and funding of technology innovations in cybersecurity, particularly the development and integration of artificial intelligence technologies, is crucial for advancing defence mechanisms and effectively countering the increasing frequency and sophistication of cyberattacks. Measures to enhance cybersecurity across the critical infrastructure providers could also be encouraged through the implementation of tax deductions, loans with prime rates, subsidies, and other incentives.
- Encourage multistakeholder cooperation, including the structured inclusion of private sector and other stakeholder voices in diplomatic forums, at the United Nations and elsewhere, responsible for establishing and upholding international expectations for responsible state behaviour online.
- Encourage and increase international cooperation among countries and between players by breaking silos, collaborating with private partners, and making use of specialised Digital Operation Centres (SOCs/DOCs) to streamline response in time of crises.
- Make cybersecurity requirements an element of government procurement contracts.
- Increase prevention measures and cybersecurity capacity building.
- Promote information sharing about threats by supporting information sharing and analysis centres (ISACs) and regional security operation centres (SOCs). Dedicated knowledge-sharing platforms could help facilitate the exchange of lessons learned, effective practices, and detailed reports of cyberattacks, enhancing the collective resilience against threats to critical infrastructures.
- Provide funding for information sharing centres and to increase cyber resilience and fighting cybercrime.

Annex I: Overview of national and regional approaches on the cybersecurity of critical infrastructures and essential services

Region	Country / regional entity	How infrastructure is defined?	What is designated as critical infrastructure?	Source
Americas	**Argentina**	**In Sept 2019, Argentina passed a resolution which defined and designated critical infrastructures (CI) and critical information infrastructures (CII).** *Critical Infrastructures are **those that are essential for the proper functioning of essential services** of society, health, safety, defence, social welfare, the economy and the effective functioning of the State, whose destruction or disturbance, total or partial, affects and/or impacts them significantly.* *CII are information technologies, operation and communication, as well as the associated information, which are vital for the operation or security of CI.*	1. Energy 2. Information and Communications Technologies 3. Transport 4. Water 5. Health 6. Food 7. Finance 8. Nuclear 9. Chemical 10. Space 11. State	Resolution 1523/2019: www.argentina.gob.ar/normativa/nacional/resolu-ci%C3%B3n-1523-2019-328599/texto Definition and designation is in Annex: www.argentina.gob.ar/sites/de-fault/files/infoleg/res1523-1.pdf Further relevant definitions: www.argentina.gob.ar/sites/de-fault/files/infoleg/res1523-2.pdf
Americas	**Brazil**	Decree No. 9,573 of 22 November 2018 approved the National Critical Infrastructure Security Policy (PNSIC), which defines **CI as facilities, services, goods and systems** whose interruption or destruction, in whole or in part, would have a serious social, environmental, economic, political, international or security impact on the state and society. Likewise, it characterises critical infrastructure security as a set of preventive and reactive measures designed to preserve or restore the **provision of services** related to CI.	1. Water 2. Energy 3. Transport 4. Communications 5. Finance 6. Biosafety and Bioprotection 7. Defence	National Policy and security of critical infrastructure: www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas-sic www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm National strategy on security of critical infrastructure: www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm National security plan of critical infrastructure: www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11200.htm

Region	Country / regional entity	How infrastructure is defined?	What is designated as critical infrastructure?	Source
Americas	**Canada**	CI refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. CI can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of CI could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence.	1. Water 2. Safety 3. Health 4. Finance 5. Transportation 6. Energy and utilities 7. Food 8. Manufacturing 9. Government 10. Communication technology	Public Safety Canada – Canada's Critical Infrastructure: www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx National Strategy for Critical Infrastructure: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf
Americas	**Chile**	Chile passed in December 2023 a Framework Law on Cybersecurity and Critical Information Infrastructure, establishing a national cybersecurity agency. Scope of the law: Requires public and private entities that qualify as providers of essential services and those that, in addition to providing Essential Services, are qualified as operators of vital importance (OIV) by the new National Cybersecurity Agency.	To be defined by the new Cybersecurity Agency.	Chile Framework Law on Cybersecurity and Critical Information Infrastructure: www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06 (Approved in December 2023)
Americas	**Colombia**	Colombia (2022) defines critical cyber infrastructure as follows: Systems and assets, physical or virtual, supported by Information and Communication Technologies, whose significant affectation would have a serious impact on the social or economic well-being of citizens, or on the effective functioning of the government or the economy. **It establishes security obligations for authorities owning critical infrastructure, or providing essential services.** The authorities, defined as holders of critical infrastructure or providing essential services, shall endeavour to have a digital security plan, protection of networks, critical cyber infrastructures, essential services and information systems in cyberspace and shall periodically carry out a digital security risk assessment. To this end, they must have the necessary rules, policies, procedures, technical, administrative and human resources to effectively manage the risk, and in compliance with the best practices and standards that may be required.	No defined sectors.	Government of Colombia normative paper on critical infrastructure: www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Region	Country / regional entity	How infrastructure is defined?	What is designated as critical infrastructure?	Source
Americas	**United States of America**	The National Institute of Standards and Technology (NIST) defines critical infrastructure as 'system and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters'.	1. Chemical sector 2. Commercial facilities sector 3. Communications sector 4. Critical manufacturing sector 5. Dams sector 6. Defence industrial base sector 7. Emergency services sector 8. Energy sector 9. Financial services sector 10. Food and agriculture sector 11. Government facilities sector 12. Healthcare and public health sector 13. Information technology sector 14. Nuclear reactors, materials and waste sector 15. Transportation systems sector 16. Water and wastewater systems	NIST critical infrastructure - Glossary | CSRC (nist.gov) Cybersecurity and infrastructure security agency – critical infrastructure sectors: Critical Infrastructure Sectors | CISA
Asia	**P. R. China**	The Security Protection Regulations for Critical Information Infrastructure (the "Regulation") was passed at the State Council executive meeting on April 27, 2021, and went into effect on Sept 1, 2021. The regulation defined the critical information infrastructure as "the key network facilities and information systems in important industries and areas such as public telecommunication and information service, energy, transport, water conservancy, finance, public service, e-government and science and technology industry for national defence, which may seriously endanger the national security, national economy, people's livelihood and public welfare once they are subject to any destruction, loss of function or data leakage."	Important network facilities and information systems in important sectors, including but not limited to: 1. Public telecommunications and information services sector 2. Energy sector 3. Transportation sector 4. Water conservancy sector 5. Finance sector 6. Public services sector 7. E-government sector 8. National defence science, technology and industry sector In accordance with the SPRCII and practice, operators of CII are usually informed by regulatory authorities that the network facilities or information systems they operate constitute CII, and the list of such CIIs is not publicly available.	Cybersecurity Law of the PRC: www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm (Chinese version only) SPRCII: www.gov.cn/gongbao/content/2021/content_5636138.htm (Chinese version only)

Region	Country / regional entity	How infrastructure is defined?	What is designated as critical infrastructure?	Source
Asia	**India**	As per the Information Technology Act 2000 (amended in 2008), CII means 'Computer Resource, the incapacitation or destruction of which, shall have debilitating impact on National Security, Economy, Public Health or Safety'.	1. Telecommunications 2. Power and energy 3. Banking and financial services 4. Transportation 5. Strategic entities 6. Government enterprises 7. Healthcare	Bank Info Security – India to Launch Critical Infrastructure Security Framework: www.bankinfosecurity.asia/india-to-launch-critical-infrastructure-security-framework-a-22282 The Information Technology Act of 2000: eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=#:~:text=%5B9th%20June%2C%202000%5D%20An,communication%20and%20storage%20of%20information%2C
Asia	**Singapore**	Under section 7(1) of the Cybersecurity Act, a CII is a computer or a computer system located wholly or partly in Singapore, necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore.	1. Energy 2. Water 3. Banking and finance 4. Healthcare 5. Transport (including land, maritime, and aviation) 6. Infocomm 7. Media 8. Security and emergency service 9. Government	Cybersecurity Act Overview www.csa.gov.sg/faq/cybersecurity-act Cybersecurity Act, Critical Infrastructure: www.csa.gov.sg/legislation/Cybersecurity-Act#:~:text=The%20CII%20sectors%20are%3A%20Energy,and%20Emergency%20Services%2C%20and%20Government.

Region	Country / regional entity	How infrastructure is defined?	What is designated as critical infrastructure?	Source
Africa	**Egypt**	Cyber warfare involves threats by nations and their sponsored groups aimed at infiltrating the critical infrastructure sectors of other countries, such as energy, telecommunications, and banking, for purposes of espionage, political and strategic gains, or purely for sabotage. It is important to note that many countries have openly declared their possession of offensive cyber capabilities as a means of self-defence against these threats. In the context of Egypt, «critical infrastructure» encompasses essential services and assets whose disruption would significantly impact national security, economic stability, public health, or safety.	1. ICT sector: It includes telecommunications networks, submarine and land cables, communications towers, communications satellites, communications control centres, telecommunications and Internet service providers. 2. Financial services sector: It includes networks and websites of banks, banking transaction, e-payment platforms, stock exchange, securities trading companies and postal financial services. 3. Energy sector: It includes systems, networks and stations that control the production and distribution of electricity, oil and gas; High Dam stations; nuclear power plants; and others. 4. Government services sector: It includes the e-government portal and websites, government agencies and institutions websites, national databases— the most important of which is the national ID database, and associated networks and websites. 5. Transportation sector: It includes air, land, sea and Nile transport. It covers all train and metro control systems, centres and networks, as well as air and sea navigation traffic networks and control systems. 6. Health and emergency aid services sector: It includes relief and emergency networks, blood banks, hospital systems and networks, health care networks and websites. 7. Information and culture sector: It includes networks, systems and websites of information and broadcasting services.	National Cybersecurity Strategy for Egypt 2023-2027: www.mcit.gov.eg/Upcont/Documents/Publications_1412024000_National_Cybersecurity_Strategy_2023_2027.pdf www.egcert.eg/wp-content/uploads/2024/02/Publications_1412024000_ar_National_Cybersecurity_Strategy_2023_2027.pdf National Cybersecurity Strategy 2017-2021: www.egcert.eg/wp-content/uploads/2023/02/strategy.pdf

Region	Country / regional entity	How infrastructure is defined?	What is designated as critical infrastructure?	Source
Africa	**Ghana**	CII constitutes assets (real/virtual), networks, systems, processes, information, and functions that are vital to the nation such that their incapacity or destruction would have a devastating impact on national security, the economy, public health and/or safety. CII may comprise a number of different infrastructures with essential interdependencies and critical information flows between them. The Cybersecurity Act of 2020 (Act 1038) defines a CII as a computer system or computer network that is essential for national security or the economic and social well-being of citizens.	1. National security and intelligence 2. Information and communication technology 3. Banking and finance 4. Energy 5. Water 6. Transport 7. Health 8. Emergency services 9. Government 10. Food and agriculture 11. Manufacturing 12. Mining 13. Education	Directive for the Protection of Critical Information Infrastructure: www.csa.gov.gh/resources/Directive_CII.pdf Cybersecurity Act of 2020: www.csa.gov.gh/resources/cybersecurity_Act_2020(Act_1038).pdf
Africa	**South Africa**	Requirements fordeclaration of infrastructure as critical infrastructure: Infrastructure qualifies for declaration as critical infrastructure, if (a) the functioning of such infrastructure is essential for the economy, national security, public safety and the continuous provision of basic public services; and (b) the loss, damage, disruption or immobilisation of such infrastructure may severely prejudice (i) the functioning or stability of the Republic; (ii) the public interest with regard to safety and the maintenance of law and order; and (iii) national security.	No defined sectors, critical infrastructures are based off the definition.	Critical Infrastructure Protection Act of 2019: www.static.pmg.org.za/Critical_Infra_Protection_Act8of2019.pdf Cybersecurity Water Policy and the Legislative Context of the Water and Wastewater Sector in South Africa: www.mdpi.com/2071-1050/13/1/291

Region	Country / regional entity	How infrastructure is defined?	What is designated as critical infrastructure?	Source
Europe	**European Union**	In Europe, there are two main directives focusing on the protection of CI and essential services, and some specialised approaches such as the one focused on the financial sector, all approved at the same time to seek coherence. The Critical Entities Resilience (CER) Directive lays down obligations to take specific measures, to ensure that essential services for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market. Moved from assets to critical entities providing essential services with Directive 2022/2557: 'Critical entities provide essential services in upholding key societal functions, supporting the economy, ensuring public health and safety, and preserving the environment.' However exact critical entities are defined by member states as follows: 'Member States will have to identify the critical entities for the sectors set out in the Critical Entities Resilience (CER) Directive by 17 July 2026. They will use this list of essential services to carry out risk assessments and to then identify the critical entities. Once identified, the critical entities will have to take measures to enhance their resilience.'	1. Energy sector, with services such as the electricity production and energy storage; 2. Transport sector, with services such as management and maintenance of airport or railways infrastructure; 3. Banking sector, with essential services such as taking deposits and lending; (This sector has an additional specific regulation on cybersecurity) 4. Financial market infrastructure sector, with services such as the operation of trading venue and of clearing systems; 5. Health sector, with distribution, manufacturing, provision of healthcare, and medical services; 6. Drinking water sector, with drinking water supply and drinking water distribution; 7. Waste water sector, with waste water collection, treatment and disposal services; 8. Digital infrastructure sector, with services such as public electronic communications networks and services, the provision and operation of internet exchange point service, domain name system, top-level domain, cloud computing and data centre; 9. Public administration sector services; 10. Space sector, with the operation of ground-based infrastructure services; 11. Production, processing and distribution of food sector, with the large-scale industrial food production and processing, food supply chain services and food wholesale distribution services.	Critical Entites Resilience (CER) Directive: www.eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557 Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2) www.eur-lex.europa.eu/eli/dir/2022/2555/oj Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA) www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554

Region	Country / regional entity	How infrastructure is defined?	What is designated as critical infrastructure?	Source
Europe	**United Kingdom**	Not everything within a national infrastructure sector is judged to be 'critical'. The UK government's official definition of CNI is: 'Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) Major detrimental impact on the availability, integrity or delivery of essential services - including those services whose integrity, if compromised, could result in significant loss of life or casualties - taking into account significant economic or social impacts; and/or b) Significant impact on national security, national defence, or the functioning of the state.'	1. Chemicals 2. Civil Nuclear 3. Communications 4. Defence 5. Emergency Services 6. Energy 7. Finance 8. Food 9. Government 10. Health 11. Space 12. Transport 13. Water	
Oceania	**Australia**	The 2023 Critical Infrastructure Resilience Strategy defines critical infrastructure as: 'those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security. Each class of critical infrastructure asset is defined by the Security of Critical Infrastructure Act 2018. A single critical infrastructure asset includes multiple parts such as premises, computers, and data, which function together as a system or network. If multiple components operate as a single system or network that meets the definition of a critical infrastructure asset, they are considered a single asset. If components operate as separate systems or networks that each meet the definition of a critical infrastructure asset, they are considered separate assets.'	1. Communications 2. Financial services and markets 3. Data storage and processing 4. Defence 5. Higher education and research 6. Energy 7. Food and grocery 8. Healthcare and medical 9. Space technology 10. Transport 11. Water and sewerage	

About the International Chamber of Commerce

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 170 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 E icc@iccwbo.org
www.iccwbo.org @iccwbo