ICC Cybersecurity Issue Brief 3: Protecting the cybersecurity of critical infrastructures and their supply chains

**THIS IS A DRAFT PAPER AND SHOULD NOT BE PUBLISHED OR SHARED OUTSIDE OF ICC MEMBERS AND COLLABORATORS**

**GUIDANCE FOR MEMBERS:** The paper aims to spotlight challenges and best practices in safeguarding critical infrastructure cybersecurity, emphasizing that industry regulation alone cannot address these challenges. The paper is accompanied by a separate document, a table of definitions and approaches, which will serve as reference for IB3, providing an overview of how countries define and designate critical infrastructure. The current draft reflects the input of the members of ICC Digital Economy Commission’s Working Group on Cybersecurity, whom we thank for the comments and feedback offered thus far.

**This is an opportunity for all members of the Commission and National Committees to offer substantive comments and/or signal any objections with the positions within the paper or the representation of countries within the table of definitions.**

Members are kindly asked to share their feedback and comments directly in track changes to the attached documents, noting the name of their organization in the name of the file, to allow the Secretariat to go through and consolidate all the input received. Please feel free to circulate this paper *within your organisation* to any interested colleagues or members but please do not share externally nor publish the paper at this point.

Please share edits with [timea.suto@iccwbo.org](mailto:timea.suto@iccwbo.org) and [meni.anastasiadou@iccwbo.org](mailto:meni.anastasiadou@iccwbo.org) by **Wednesday, 24 April**.

## ****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 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 on short term and are therefore deemed to need special physical and digital protections. This may include sectors like energy, water, heat, 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 service* 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]](#footnote-2)

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 organizational 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. 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]](#footnote-3)

[PLACEHOLDER: A paragraph will be added here to summarize the main recommendations of the paper, once written]

## ****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]](#footnote-4) 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 recognized 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[[4]](#footnote-5) aligns with national strategic approaches and provides guidance for decision-making. It also recommends prioritizing 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 emphasizes the importance of strengthening risk management through the identification and prioritization of critical assets, periodic cybersecurity risk assessments, and the allocation of resources to maximize 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 include:

* + In Europe attacks on Estonian organizations including the Parliament, banks, ministries, newspapers, and others as early as 2007 were a wakeup call helping the country improve their cyber-defence tools.[[5]](#footnote-6) 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]](#footnote-7) A large number of similar threats were reported in the 2008-2014 period.[[7]](#footnote-8) Most recently a number of attacks were reported in Ukraine (such as wiper ransomware) following the conflict with Russia.[[8]](#footnote-9)
* 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]](#footnote-10)
* In May 2021 the Colonial pipeline ransomware attack forced all business operations to stop.[[10]](#footnote-11)
* In Central and South America in January 2024 the Trigona attack on Claro operations caused over a week of disruption to services.[[11]](#footnote-12)

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 or Operational Technology brings an explosion of potential new risks deriving from the joint effect of digital vulnerabilities and the complexity of the physical world. One example of this was the case of Stuxnet,[[12]](#footnote-13) by which a specialized 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 destabilizing 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]](#footnote-14) to diverse vulnerabilities and attacks on the software and digital services supply chain, affecting organisations in different countries. One example is an incident occurred in 2017, when the shipping giant Maersk, based in Copenhagen, Denmark became a victim of the NotPetya ransomware attack.[[14]](#footnote-15) 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. Recently Log4shell,[[15]](#footnote-16) SolarWinds,[[16]](#footnote-17) and Ivanti[[17]](#footnote-18) are other examples.

Harmonized 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.

[PLACEHOLDER: A visual or table to be added here with an overview of various jurisdictions’ take on CI – for the time being please add your observations to the table provided in a separate document]

The first step towards finding common agreement on terminology for critical infrastructure is convergence in using globally recognized, widely utilized 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 utilized for complying with global financial regulations. Utilizing 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.

## ****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 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 decentralized protocols, insufficient levels of encryption and protection in protocols and services, insufficient roots of trust in encryption capabilities...)
* 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 organizations 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 organizations and insider threats, each actor is driven by distinct motivations that can extend beyond financial gains, encompassing geopolitical influence or event ideological pursuits.

**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.[[18]](#footnote-19) 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 organization 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 five million guests.[[19]](#footnote-20)

**State-nexus threat groups or Advanced Persistent Threats (APTs)**

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 primary objective is espionage and revenue generation, and they target both other countries and private organizations to obtain sensitive data, funding, or military strategies.[[20]](#footnote-21) Examples of such threats include Stuxnet mentioned above, GhostNet reported to have compromised the devices of political, economic, and media targets in nearly 103 countries[[21]](#footnote-22), Helix Kitten whose major targets included organizations in aerospace, energy, financial, government, hospitality, and telecommunications, mostly in the Middle East[[22]](#footnote-23) or the more recently identified Flax Typhoon[[23]](#footnote-24) claimed to gain and maintain long-term access to organizations’ 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.

**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]](#footnote-25) 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 specialized cybercriminal organizations, more resilient to takedowns and prosecution. This trend has led to a significant rise in the number of criminals utilizing ransomware and the overall magnitude of cybercrimes these days.[[25]](#footnote-26) Examples include the Lazarus Group behind the WannaCry ransomware attack[[26]](#footnote-27), REvil mostly known for the Kaseya attack and reportedly responsible for 37% of ransomware attacks in 2021[[27]](#footnote-28) or Lapsus$ pursuing attacks against companies and government agencies with social engineering tactics.[[28]](#footnote-29)

**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]](#footnote-30)

**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 emphasize 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]](#footnote-31)

**Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) 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 websiteor online servers of critical infrastructure unavailable.[[31]](#footnote-32) 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]](#footnote-33) The focus may be on overwhelming communication networks, rendering them unable to coordinate and respond effectively.[[33]](#footnote-34)

**Targeted Exploitation of Industrial Control Systems**

Cyber threats to critical infrastructure often involve the targeted exploitation 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.[[34]](#footnote-35)

**Sophisticated Malware**

Cyber threats to critical infrastructure often involve sophisticated malware and APTs. 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.[[35]](#footnote-36)

**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.[[36]](#footnote-37)

**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 organizations and threatening to release it publicly unless a payment is made, they also target organizations’ 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 organizations and their suppliers, vendors, and third-party service providers vital to the supply chain.[[37]](#footnote-38) One supply chain attack taxonomy has been proposed by ENISA, see figure *[figure number to be added later]* containing four parts: (i) attack techniques used on the supplier, (ii) assets attacked in the supplier, (iii) attack techniques used on the customer, (iii) 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. [[38]](#footnote-39)

A screenshot of a computer

Description automatically generated

*Figure XX: ENISA taxonomy for supply chain attacks.*

**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.[[39]](#footnote-40) 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 and handling emergency of cyberattack.[[40]](#footnote-41) 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 critical infrastructure 's operations may expand across national boundaries, it is important to recognize 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.[[41]](#footnote-42)

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.[[42]](#footnote-43) 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 jurisdictions such as the EU and Taiwan, 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.[[43]](#footnote-44) Conversely, certain jurisdictions, like Japan, do not explicitly identify critical infrastructure providers.[[44]](#footnote-45) 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.[[45]](#footnote-46) In sum, a standardized framework is recommended for defining and implementing measures for the operation of the critical infrastructure and international cooperation.

**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 cognizant 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.[[46]](#footnote-47)

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.

## ****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 organizations (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 cyberthreats, 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 Team (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.).

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 minimize 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 (ENS in Spain for the public sector, TSA in UK for communication service providers, to name a few) to bring down to earth more generic framework and to ease further compliance check by regulatory bodies.

All of these should be seen as reference frameworks, and appropriate mapping across them 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 ISP 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 generalize. 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%.[[47]](#footnote-48) In the EU, it is 80%.[[48]](#footnote-49) In the UK, approximately 50% of critical infrastructure is owned and operated privately[[49]](#footnote-50), while in many other markets, such China 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 section XX and figure YY. 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 WEF State of cyber-security report 2024 identified among others a growing cyber-resilience gap between large and SME companies 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.[[50]](#footnote-51)

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,[[51]](#footnote-52) 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[[52]](#footnote-53) 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.[[53]](#footnote-54) Total economic loss from supply chain attacks, albeit a fraction of aggregate cost of cyber-attacks[[54]](#footnote-55) 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 8 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 organizations with mature security programs, developers have adopted practices, such as consistent code reviews, disciplined internal vulnerability management and aggressive patching protocols, especially concerning third party dependencies.[[55]](#footnote-56)

**Industry best practices**

Regarding the protection of supply chain, the use of best practices like the ones below could be considered:[[56]](#footnote-57) [[57]](#footnote-58)

1. **Focus on a set of priority security requirements** based on an assessment of risk, a short list instead of overloading 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](https://cybertechaccord.org/zero-trust-once-again/), 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 programs, 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 minimize 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.

In the context of ICT supply chain risk management, for example, a supply chain risk-management process[[58]](#footnote-59) 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 recognize 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[[59]](#footnote-60) 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 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 visualized in figure XX.

A diagram of a software company

Description automatically generated

*Figure XX* Securing software supply chain based on Ericsson Security Reliability Model

**Open-source software security**

Many ICT vendors and communication service providers leverage open-source software 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 OpenSSF (Open Source Security Foundation) is another organization that is promoting standards for assurance of open source across the industry.[[60]](#footnote-61)

Use of open-source software requires a higher level of due diligence which organizations can implement by applying industry best practices for supply chain management, secure software development, and secure software maintenance. There are government and industry organizations available to help, including DARPA AIxCC[[61]](#footnote-62), the US Department of Commerce’s National Institute of Standards (NIST), The Linux Foundation, and 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[[62]](#footnote-63), 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 utilized 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 recognized 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.

GSMA and NIST have developed Internet of Things (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 organizations to “gain assurance about the cybersecurity of their organisation’s supply chain.[[63]](#footnote-64) The guidance describes how organizations are exposed to vulnerabilities and cyberattacks through their supply chain and defines expected outcomes and key steps to help organizations 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.

There are similar initiatives underway in other markets which resemble the common provisions in the US, EU and UK legislation and regulation, such as the guidance by the Canadian Centre for Cyber Security on protecting organizations from software supply chain threats[[64]](#footnote-65) or by the New Zealand National Cyber Security Centre on supply chain cyber security[[65]](#footnote-66). Nonetheless, much remains to be done.

The aim should be to achieve harmonized requirements across markets based on business best practices and international standards. Many past efforts to harmonize 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 US and EU to streamline incident reporting obligations should be further encouraged and also over time geographically broadened in relevant international forums.[[66]](#footnote-67)

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. This involves i) disrupting cyber threat actors, ii) prosecuting cybercrimes more effectively, and iii) 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 summarized 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:
   1. Alignment across supply chains on the development and use of technical security standards.
   2. Alignment on and implementation of risk-based security risk management frameworks for the suppliers and the operators of critical infrastructure and essential services.
   3. 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 minimizing 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 organization’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[[67]](#footnote-68) 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:

* + 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.
* A holistic national policy framework is more likely to be effective if co-ordinated 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.

**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 modernization 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.
* Encourage multistakeholder and international cooperation. Increase cooperation among countries and between players by breaking silos, collaborating with private partners, and making use of specialized 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).
* Provide funding for information sharing centres and to increase cyber resilience and fighting cybercrime.

**Annex I: Regional experiences**

**Europe**

Europe is one of the regions with the most mature cybersecurity policies, with cybersecurity strategies, independent cyber agencies with clearly defined technical competencies, regulatory frameworks, and cybersecurity guidelines to improve practices, a certification framework, cooperation processes and programmes for innovation, and supporting cyber capacities, deployment, and skill development. Based on lessons learnt and on the new cyber threat landscape, Europe is now updating them. To name a few of the most important future frameworks:

* + The NIS2 directive on measures for a high common level of cybersecurity across the Union will apply to companies considered as essential or important in 18 critical sectors, as of 18 October 2024. NIS2 expands the scope of the cybersecurity rules to new sectors and entities, to further improve the resilience and incident response capacities. Closing the gap in supply chain security and increasing coordination of incidents reporting and response remains a challenge.
  + Aligned with the NIS2 directive the Critical Entities Resilience Directive (CER) lays down obligations on EU Member States 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. Member States will have to identify the critical entities for the sectors set out in the CER Directive by 17 July 2026.
  + The proposal on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act (CRA), with cybersecurity rules towards more secure hardware and software products. Resilience will increase through a better allocation of responsibility for cybersecurity along all the value chain and with harmonised requirements. It will come into force 24 months after its approval.
  + The recently approved DORA regulation on digital operational resilience for the financial sector, applicable from January 2025, will also test the water 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.

**South America**

In September 2023, in Colombia (and other countries of the region), more than 50 state entities and private companies were hit by a ransomware attack against Internet service provider IFX Networks, with a major impact in public services. This has again highlighted the importance of adequate cybersecurity measures for the resilience of government services, the importance of security clauses in contracts beyond the lowest bidder price approach, and the need for an appropriate legal framework.

In 2022, Costa Rica became a showcase and a lesson to increase prevention and security capacity building for all countries. Costa Rica had to declare a state of emergency, when its government agencies fell victim to a ransomware operation from a Russian cybercrime gang, which caused overnight paralysis of critical government services (e.g. customs operations, non-payment of teachers’ salaries, loss of access to patient health records or medical appointments). Interstate security cooperation and assistance requested from a number of countries, including the United States, Spain, and Israel, became a key element in addressing the problems. After this hard learning, Costa Rica is establishing itself as a regional leader in cybersecurity.

1. US: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>; Europe: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>; List of Essential Services: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202302450> [↑](#footnote-ref-2)
2. [↑](#footnote-ref-3)
3. Executive Decree No. 43542-MP-MICITT de 2022 [↑](#footnote-ref-4)
4. https://www.micitt.go.cr/el-sector-informa/avanza-proceso-de-implementacion-de-la-estrategia-nacional-de-ciberseguridad [↑](#footnote-ref-5)
5. <https://www.bbc.com/news/39655415> [↑](#footnote-ref-6)
6. https://ccdcoe.org/uploads/2018/10/legalconsiderations\_0.pdf [↑](#footnote-ref-7)
7. https://ccdcoe.org/uploads/2018/10/Ch08\_CyberWarinPerspective\_Weedon.pdf [↑](#footnote-ref-8)
8. Example of cyberattack against energy infrastructure. https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology [↑](#footnote-ref-9)
9. <https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-how-the-modest-bowman-avenue-dam-became-the-target-of-iranian-hackers/> [↑](#footnote-ref-10)
10. <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know> [↑](#footnote-ref-11)
11. <https://commsrisk.com/ransomware-attack-hits-claro-across-latin-america/> [↑](#footnote-ref-12)
12. <https://spectrum.ieee.org/the-real-story-of-stuxnet> [↑](#footnote-ref-13)
13. <https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/> [↑](#footnote-ref-14)
14. [NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million (forbes.com)](https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/?sh=2cf6bdf14f9a). [↑](#footnote-ref-15)
15. <https://www.ibm.com/topics/log4shell> [↑](#footnote-ref-16)
16. <https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T> [↑](#footnote-ref-17)
17. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b> [↑](#footnote-ref-18)
18. ENISA, ENISA ETL2020 - [Insider Threat, p.1.](https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-insider-threat/@@download/fullReport) (Last visited: Jan 23, 2024) [↑](#footnote-ref-19)
19. <https://www.bbc.com/news/technology-54748843> [↑](#footnote-ref-20)
20. ENISA, ENISA Threat Landscape 2023, available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport> (last visited: Mar. 13, 2024). [↑](#footnote-ref-21)
21. <https://www.infosecinstitute.com/resources/threat-intelligence/ghostnet-part-i/#gref> [↑](#footnote-ref-22)
22. <https://www.wired.com/story/apt-34-iranian-hackers-critical-infrastructure-companies/> [↑](#footnote-ref-23)
23. <https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/> [↑](#footnote-ref-24)
24. Two years after WannaCry, a million computers remain at risk, TechCrunch, available at: <https://techcrunch.com/2019/05/12/wannacry-two-years-on/#:~:text=Two%20years%20on%2C%20the%20threat,according%20to%20the%20latest%20data>. (last visited: Jan 30, 2024) [↑](#footnote-ref-25)
25. National Cyber Security Centre, Ransomware, extortion and the cybercrime ecosystem, available at: <https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem> (last visited: Jan 23, 2024) [↑](#footnote-ref-26)
26. <https://www.nccgroup.com/us/the-lazarus-group-north-korean-scourge-for-plus10-years/> [↑](#footnote-ref-27)
27. <https://newsroom.ibm.com/2022-02-23-IBM-Report-Manufacturing-Felt-Brunt-of-Cyberattacks-in-2021-as-Supply-Chain-Woes-Grew> [↑](#footnote-ref-28)
28. <https://www.theverge.com/22998479/lapsus-hacking-group-cyberattacks-news-updates> [↑](#footnote-ref-29)
29. Anonymous declared a ‘cyber war’ against Russia. Here are the results, CNBC, available at: <https://www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html> (last visited: Jan 30, 2024) [↑](#footnote-ref-30)
30. Ericsson, Deciphering the evolving threat landscape: security in a 5G world: <https://www.ericsson.com/en/blog/2023/10/deciphering-the-evolving-threat-landscape-security-in-a-5g-world> [↑](#footnote-ref-31)
31. Fortinet, What Is the Difference Between DoS Attacks and DDoS Attacks? Available at: <https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos#:~:text=A%20denial%2Dof%2Dservice%20(,to%20flood%20a%20targeted%20resource>. (last visited: Feb 27, 2024) [↑](#footnote-ref-32)
32. Id. [↑](#footnote-ref-33)
33. Please note that 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, available at: <https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps> (last visited: Feb 27, 2024) [↑](#footnote-ref-34)
34. David E. Sanger and Julian E. Barnes, U.S. Hunts Chinese Malware That Could Disrupt American Military Operations, The New York Times, available at: <https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html> (last visited: Feb 27, 2024) [↑](#footnote-ref-35)
35. GReAT, APT trends report Q3 2023, SECURELIST by Kaspersky, available at: <https://securelist.com/apt-trends-report-q3-2023/110752/> (last visited: Feb 27, 2024) [↑](#footnote-ref-36)
36. . <https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html> [↑](#footnote-ref-37)
37. Bart Lenaerts-Bergmans, What is a supply chain attack? available at: <https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/> (last visited: Jan 28, 2024) [↑](#footnote-ref-38)
38. For instance, 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 organizations. Cyberint, The Weak Link: Recent Supply Chain Attacks Examined, available at: <https://cyberint.com/blog/research/recent-supply-chain-attacks-examined/> (last visited: Jan 28, 2024) [↑](#footnote-ref-39)
39. Anup K. Ghosh, Michael J. Del Rosso, The Role of Private Industry and Government in Critical Infrastructure Assurance, available at: <https://gost.isi.edu/cctws/delroso-ghosh.PDF> (last visited: Jan 29, 2024) [↑](#footnote-ref-40)
40. For instance, 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.

    *See* Mary Brooks, Annie Fixler & RADM (Ret.) Mark Montgomery, Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure, p.9, available at: <https://cybersolarium.org/csc-2-0-reports/revising-public-private-collaboration-to-protect-u-s-critical-infrastructure/> (last visited: Feb 27, 2024) [↑](#footnote-ref-41)
41. For example, 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. *See* Gregory C. Allen, China Is Striking Back in the Tech War with the U.S. TIME, available at: <https://time.com/6295902/china-tech-war-u-s/> (last visited: Feb 27, 2024) [↑](#footnote-ref-42)
42. [↑](#footnote-ref-43)
43. Cyber Security Management Act; Directive on Security of Network and Information Systems, European Commission, available at: <https://ec.europa.eu/commission/presscorner/detail/el/MEMO_16_2422> (last visited: Jan 30, 2024) [↑](#footnote-ref-44)
44. OneTrust Data Guidance, Japan: Cybersecurity, available at: <https://www.dataguidance.com/opinion/japan-cybersecurity> (last visited: Jan 30, 2024) [↑](#footnote-ref-45)
45. ICLG, Cybersecurity Laws and Regulations Japan 2024, available at: <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/japan> (last visited: Jan 30, 2024) [↑](#footnote-ref-46)
46. Good Governance for Critical Infrastructure Resilience-4. [Critical infrastructure resilience case-study: Electricity transmission and distribution in Finland](https://www.oecd-ilibrary.org/sites/93ebe91e-en/index.html?itemId=/content/component/93ebe91e-en), OECD (Last visited: Jan 29, 2024) [↑](#footnote-ref-47)
47. Government Accountability Office, The Department of Homeland Security’s (DHS) Critical Infrastructure Protection Cost-Benefit Report, June 26, 2009. [↑](#footnote-ref-48)
48. <https://www.gisreportsonline.com/r/europe-critical-infrastructure/> [↑](#footnote-ref-49)
49. <https://nic.org.uk/themes/design-funding/>) [↑](#footnote-ref-50)
50. <https://www.austrac.gov.au/business/core-guidance/amlctf-programs/implement-risk-management-process> [↑](#footnote-ref-51)
51. <https://www.reversinglabs.com/blog/a-partial-history-of-software-supply-chain-attacks> [↑](#footnote-ref-52)
52. <https://www.statista.com/statistics/1375128/supply-chain-attacks-software-packages-affected-global/> [↑](#footnote-ref-53)
53. <https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022> [↑](#footnote-ref-54)
54. <https://www.weforum.org/publications/global-cybersecurity-outlook-2024/> [↑](#footnote-ref-55)
55. <https://go.snyk.io/2023-supply-chain-attacks-report-dwn-typ.html?aliId=eyJpIjoidFd0SVpwb0R6M2VNeUMrMyIsInQiOiJGRUE3VFdwTDB4Tk95TzkzTERadzRRPT0ifQ%253D%253D> [↑](#footnote-ref-56)
56. RSAC ESAF Report: How Top CISOs Are Transforming Third-Party Risk Management <https://email.rsaconference.com/p/7K6E-7LN/nur-48-2023esaf-form> [↑](#footnote-ref-57)
57. Cybersecurity Tech Accord: Best practice alignment for supply chain security across standards and regulatory frameworks <https://cybertechaccord.org/best-practice-alignment-for-supply-chain-security-across-standards-and-regulatory-frameworks/> [↑](#footnote-ref-58)
58. <https://www.ericsson.com/en/security/ericssons-security-reliability-model> [↑](#footnote-ref-59)
59. <https://www.synopsys.com/glossary/what-is-devsecops.html> [↑](#footnote-ref-60)
60. [Open Source Security Foundation – Linux Foundation Projects (openssf.org)](https://openssf.org/) [↑](#footnote-ref-61)
61. [aicyberchallenge.com](https://aicyberchallenge.com/) [↑](#footnote-ref-62)
62. [CISA Open Source Software Security Roadmap](https://www.cisa.gov/sites/default/files/2024-02/CISA-Open-Source-Software-Security-Roadmap-508c.pdf) [↑](#footnote-ref-63)
63. <https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security> [↑](#footnote-ref-64)
64. <https://www.cyber.gc.ca/en/guidance/protecting-your-organization-software-supply-chain-threats-itsm10071> [↑](#footnote-ref-65)
65. <https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf> [↑](#footnote-ref-66)
66. [Comparative Assessment of the DHS Harmonization of Cyber Incident Reporting to the Federal Government Report and the Rules on Incident Reporting in the NIS 2 Directive | Shaping Europe’s digital future (europa.eu)](https://digital-strategy.ec.europa.eu/en/library/comparative-assessment-dhs-harmonization-cyber-incident-reporting-federal-government-report-and) [↑](#footnote-ref-67)
67. [Enhancing the security of communication infrastructure | OECD Digital Economy Papers | OECD iLibrary (oecd-ilibrary.org)](https://www.oecd-ilibrary.org/science-and-technology/enhancing-the-security-of-communication-infrastructure_bb608fe5-en) page 38 -40. [↑](#footnote-ref-68)