OECD GOING DIGITAL TOOLKIT

POLICY NOTE

Enhancing the digital security of critical activities

OECD
BETTER POLICIES FOR BETTER LIVES

going digital

This Toolkit note was written by Laurent Bernat. It was reviewed by the OECD Working Party on Security in the Digital Economy (SDE) and the OECD Committee on Digital Economy Policy (CDEP) and it was declassified by the CDEP on 31 August 2021. The note was prepared for publication by the OECD Secretariat.

This Toolkit note is a contribution to the OECD Going Digital project, which aims to provide policy makers with the tools they need to help their economies and societies thrive in an increasingly digital and data-driven world.

For more information, visit *www.oecd.org/going-digital*.

#GoingDigital

Please cite this publication as:

Bernat, L. (2021), "Enhancing the digital security of critical activities", *Going Digital Toolkit Note*, No. 17, *https://goingdigital.oecd.org/data/toolkitnotes/No17_ToolkitNote_DigitalSecurity.pdf*.

Note to Delegations:

This document is also available on O.N.E. under the reference code:

DSTI/CDEP/SDE(2020)14/FINAL.

Table of Contents

Figures

Boxes

Enhancing the Digital Security of Critical Activities

The digital transformation of critical activities such as the delivery of water, energy, healthcare, telecommunications, and banking services increasingly exposes them to cybersecurity threats, which can affect the health, safety, and security of citizens, the functioning of essential services, or economic and social prosperity more broadly. This Toolkit note introduces key concepts, such as critical activities, critical information infrastructure (CII), cybersecurity and digital security risk management, and helps policy makers identify what needs to be protected and what types of measures operators of critical activities should take. It further discusses the institutional framework to develop and supervise policies to enhance the digital security of critical activities, including trust-based partnerships, and provides a selection of policy approaches from a range of jurisdictions in the Annex.

Digital technologies foster social progress, facilitate innovation, enhance productivity, and improve many goods and services' effectiveness, to name a few of their benefits. They have become so pervasive across value and supply chains that most economic and social activities have become digitally dependent. Among these activities, some are critical to the health, safety, and security of citizens; the effective functioning of essential services; or economic and social prosperity more broadly. Examples of such critical activities include the distribution of water and energy, as well as the provision of healthcare, telecommunications, banking, transport, and government services.

Over the last ten years, critical activities have been increasingly exposed to digital security threats, a trend that the current digital transformation is accelerating. The anticipated benefits from smart cities, digitally- enhanced power grids and healthcare are steering the adoption of disruptive technologies such as big data, artificial intelligence, Internet of Things devices and 5G networks. Although promising, these technologies are increasing the complexity of digital ecosystems that support critical activities. The attack surface[1] of operators of critical activities grows in proportion to the expanding amounts of data, hardware, software, and network infrastructures they have to manage and that can never be considered entirely secure, in particular as attackers increasingly leverage digital supply chains to achieve their nefarious goals.

At the same time, digital security threats have grown in number and sophistication. While robust statistical evidence is scarce in this area, qualitative empirical evidence is clear. Malicious actors are increasingly innovative. Criminals attack and paralyse hospitals, government agencies and cities with ransomware, including during the COVID-19 pandemic. Geopolitical tensions extend to the digital environment, adding States or State-sponsored actors with quasi-unlimited resources to the list of possible threat sources. Security researchers repeatedly identify new and sophisticated malicious code ("malware") specially designed to target critical activities, such as Havex, DragonFly, Black Energy, Grey Energy, Triton, and Industroyer, to name a few.

The possibility for digital security incidents to lead to physical damages is no longer theoretical: digital security attacks destroyed nuclear centrifuges in Iran, and generated massive physical damages in a German steel mill in 2014, as well as power outages in Ukraine in 2015 and 2017. Furthermore, the NotPetya incident in 2017 demonstrated that digital security attacks can significantly disrupt operations and supply chains for several days in areas such as global containers logistics (Maersk) and pharmaceutical production (Merck). In 2021, a cyber attack forced Colonial Pipeline Company to shut down the largest

[1] An attack surface is the total sum of potential vulnerabilities that can be exploited to carry out a security attack.

pipeline in the United States for six days, leading to fuel shortages across the East Coast.

This combination of increased digital dependency of and threats to critical activities presses governments to shift gears and adopt innovative policies to strengthen the digital security of critical activities. However, strengthening digital security can introduce significant costs and other constraints on operators of critical activities. A key policy challenge is to ensure that policy measures focus on what is critical for the economy and society, without imposing unnecessary burdens on the rest, and without undermining the benefits from digital transformation in critical sectors through constraints that would unnecessarily restrict the use and openness of digital technologies.

This Toolkit note introduces key concepts, such as critical activities, critical information infrastructure (CII), cybersecurity and digital security risk management, and helps policy makers identify what needs to be protected and what types of measures operators of critical activities should take. It further discusses the institutional framework to develop and supervise policies to enhance the digital security of critical activities, including trust-based partnerships, and provides a selection of policy approaches from a range of jurisdictions in the Annex.

Understanding key concepts

Critical activities

Box 1 introduces the OECD definition of critical activity. Countries use different terminology to refer to critical activities, such as "critical functions" (CISA, 2021[5])) or "essential services" (European Union, 2016[6]). In many instances, they also refer to "critical infrastructure".

The notion of critical infrastructure emerged in the late 1990s, as some OECD countries started to adopt critical infrastructure protection (CIP) policies. These policies typically considered critical infrastructure sectors such as energy, finance, telecommunications or public health.

Progressively, the need to develop policies to protect information systems and networks that support such critical infrastructure sectors became increasingly clear. Around 2008, it seemed natural to call these ICT assets "critical information infrastructure" (CII), as if they formed an additional critical infrastructure sector. However, although quite popular among experts, the concept of CII has rarely been used to develop domestic policy frameworks. This may be due to the difficulty to delineate CII in practice. For example, the Internet can be considered as being part of the CII because most operators of other critical infrastructures rely on it, such as banks, hospitals or energy distributors. However, these operators also rely on their internal critical information systems and networks, which therefore are also part of the CII.

Some parts of these information systems and networks may be internal to the operators of critical infrastructure, i.e. "on-premises", but others may be "in the cloud", i.e. on the Internet, and owned and managed by third parties, potentially in other jurisdictions. This combination of shared and isolated, as well as internal and external technical components makes CII difficult to represent and more complex than the more traditional "critical infrastructure" sectors upon which the CII concept was inspired.

In 2019, the OECD agreed to simplify the framework established in its 2008 Recommendation on the protection of critical information infrastructure by focusing on the need to enhance the digital security of critical activities, i.e. encourage operators of critical activities to better manage digital security risk.

Box 1. What is a critical activity?

A critical activity is an economic and social activity, the interruption or disruption of which would have serious consequences on the health, safety, and security of citizens; or the effective functioning of services essential to the economy and society, and of the government; or economic and social prosperity more broadly (OECD, 2019[4]). The latter type of critical activities includes those that are essential for prosperity without being necessarily critical to the functioning of the economy and society, nor affecting the health, safety and security of citizens. For example, car manufacturing or mining, in a country where such activities would represent a significant share of the GDP.

The notion of critical activity (sometimes called critical functions or essential services) is different from that of critical infrastructure because it focuses on the risk to the delivery of the service rather than to the assets on which the delivery of the service relies.

Digital security

There are many technical definitions of digital security, which is sometimes also called cyber security, information security, computer security, etc. From the perspective of the OECD, digital security is an economic and social challenge rather than only a technical issue. It can be viewed as the set of measures to manage digital security risk for prosperity. The OECD *Recommendation on digital security risk management for economic and social prosperity* ("Security Recommendation") and its Companion document provide more details about digital security risk and its management (OECD, 2015[7]).

Digital security risk

Digital security risk is the detrimental effect that digital security *incidents* can have on economic and social activities. A digital security incident is an event

that can disrupt the availability, integrity and confidentiality ("AIC triad") of hardware, software, networks or data that support these activities.

Digital security risk is generally represented as the combination of the *likelihood* that digital security incidents affect an economic and social activity, with the *severity* of consequences that such incidents can create to stakeholders. Stakeholders include:

- The operator of the activity by damaging its operational, physical, financial, or reputational assets (e.g. an electric utility's power stations are shut down by an attack);
- Businesses, governments and individuals who rely on the delivery of the disrupted activity such as clients or users (e.g. citizens affected by the resulting black-out);
- The society more broadly, for example if the scale of the disruption is very large (e.g. all economic activities are affected in the region, or the disruption cascades to other sectors such as transports and health care).

Digital security risk is an economic and social challenge caused by the possibility of incidents taking place at the technical level. The technical aspects of security incidents, such as the use of malware, phishing and other techniques, the corruption of data, unavailability of servers, breaches of confidentiality, and so on, should not mask the economic and social nature of the risk.

Digital security risk management

Digital security risk management is a business-driven (as opposed to only technology-driven) decision making process.

Digital security risk management has two important aspects:

- While digital security can reduce the risk to an acceptable level, it cannot entirely eliminate it. A certain level of *residual risk* must always be taken, which means that incidents can happen and create damages despite all the measures taken. The acceptable level of risk is known as the *risk appetite* or *risk tolerance* of the party managing the risk. When the activity at stake is critical to the economy and society, the residual risk is taken by the society as a whole, therefore the risk tolerance cannot only be set by the operator of the critical activity. This is the main rationale for the adoption of public policies to protect critical infrastructure and strengthen the digital security of critical activities: they set the level of risk that society can accept and that operators can use to adjust risk management accordingly.
- Digital security measures are not neutral with respect to the activity they aim to protect. They can create different kinds of barriers and constraints such as financial cost, lower capacity to evolve and innovate,

increased complexity, reduced performance, openness, convenience and usability, as well as challenges to privacy and freedom of expression. These constraints and adverse effects of security can be addressed and mitigated, but at a cost. Stakeholders' main digital security challenge is to ensure that digital security both protects and supports economic and social activities: how much security is enough to reduce the risk to an acceptable level, without undermining the activity itself?

Digital security risk management is the methodology to select security measures that are appropriate to and commensurate with the risk, are aligned with the risk tolerance, support the economic and social activities at stake, and will not undermine these activities, for example, by inappropriately closing the environment or limiting the possibility of taking advantage of ICTs to innovate and gain productivity.

To manage risk, stakeholders first make a risk assessment for each of their activity, then make a business-led decision to treat the risk, namely decide on what to do with the risk in light of their risk appetite/tolerance. They can take it and face the possible consequences, avoid it by not carrying out the activity, transfer it for example by purchasing insurance, or reduce it by adopting security and resilience measures. Resilience measures are key as they ensure that the activity can continue despite the occurrence of incidents. Stakeholders may also treat the risk by innovating and redesigning the activity to reduce its risk exposure. As digital security risk is dynamic, risk management must be systematic and cyclical.

Making policies to enhance the digital security of critical activities

From the perspective of the OECD, the overarching challenge for enhancing the digital security of critical activities is to develop policies that encourage, and in some countries require, operators of critical activities to strengthen digital security, without creating unnecessary burdens that would inhibit or reduce their ability to realise the full potential of digital transformation. Such policies need to be consistent with the principles of the OECD Security Recommendation, including with regards to human rights and fundamental values (Box 2).

Box 2. Human rights and fundamental values in the OECD Security Recommendation

The Security Recommendation includes 8 principles to guide the development of digital security policies and the implementation of a risk-based digital security approach. The third principle focuses on human rights and fundamental values (see

below). Other principles include: 1. Awareness, skills and empowerment; 2. Responsibility; 4. Co-operation; 5; Risk assessment and treatment cycle; 6. Security measures; 7. Innovation; 8. Preparedness and continuity.

All stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values.

Digital security risk management should be implemented in a manner that is consistent with human rights and fundamental values recognised by democratic societies, including the freedom of expression, the free flow of information, the confidentiality of information and communication, the protection of privacy and personal data, openness and fair process. Digital security risk management should be based on ethical conduct which respects and recognises the legitimate interests of others and of the society as a whole. Organisations should have a general policy of transparency about their practices and procedures to manage digital security risk.

Source: (OECD, 2015[7]).

Identifying what to protect

Policies to enhance the digital security of critical activities aim primarily at encouraging public and private operators of these activities, such as banks, hospitals, water and energy distributors, telecommunication network providers, airports, rail companies, etc., to better manage digital security risk. Targeting too many operators that are not truly vital to the delivery of the critical activities at stake would impose unnecessary burdens on large parts of the economy. Targeting too few would not sufficiently protect the economy. Therefore, governments need a process to identify which operators should be targeted by their policies.

To determine which operators the policy should target, governments can build upon an existing framework to protect their critical infrastructure. In lack of such a framework, they have to develop a methodology from scratch. The first step is the development of a national risk assessment covering all economic and social activities. On the basis of this assessment, and working with relevant public and private actors, the government identifies critical activities and the operators of these critical activities. Different countries have different methodologies to do so, taking into account different thresholds or criteria of criticality (e.g. possible number of users or citizens impacted by an incident). In 2020, the European Commission proposed to use a simple criteria to identify operators of essential services across the Union in the future version of the EU Directive on security of network and information systems (NIS Directive) (Box 3).

Box 3. Towards a simplification of the identification of operators in the NIS 2.0 Directive

The 2016 NIS Directive promotes a risk management culture among companies or other entities providing essential services defined as "operators of essential services" (European Union, 2016[6]). Operators which fall in the scope of the Directive are required to take appropriate and proportionate technical and organisational measures to manage the risks posed to their security of network and information systems and to notify serious incidents to competent authorities. To implement the Directive, EU members identified operators of essential services in their territories. According to the European Commission, EU Members developed a variety of methodologies to identify operators, define essential services and set thresholds. This situation creates complexity for operators whose activities span across multiple jurisdictions. It is nonetheless necessary to recognize the importance of sectoral and national specificities, especially when pertaining to matters of national security.

Released in December 2020, the European Commission's proposal for a revised "NIS 2 Directive" suggests eliminating differences between EU members by establishing a clear size-cap rule whereby all medium (above 50 employees and with an annual turnover above EUR 10 million) and large enterprises operating within the sectors listed in the proposal's annex would fall within scope of the new Directive. The proposal also distinguishes essential from important entities, which would be subject, respectively, to an *ex ante* and *ex post* supervisory regime. At the time of writing, the proposal for the NIS Directive 2.0 is being negotiated in the Council of the European Union.

Source: (European Commission, 2020[8]; European Commission, 2019[9]).

Measures for operators of critical activities

In most countries, there is a recognition that operators are responsible for the digital security of their activities. However, countries generally agree that governments' intervention is justified on the grounds that governments have some responsibility to determine the level of risk that the society can tolerate with respect to critical activities, and ensure the continuity of these activities.

The nature of governments' intervention takes many forms and uses many tools including standards' promotion, legal obligations, regulation, co-regulation, encouragement of self-regulation, crisis management assistance and technical support, among others. Over the last five years, there has been a trend towards the adoption of mandatory regulation, largely driven by the implementation of the 2016 NIS Directive in the European Union, according to which EU members had to create compliance requirements for operators of essential services (European Union, 2016[6]). Nevertheless, some other countries such as Canada and the United States favour a voluntary approach whereby

they provide support and guidance to operators without establishing mandatory requirements. According to the Japanese cybersecurity strategy, the government provides guidance to operators of critical activities rather than mandatory obligations (Government of Japan, 2018[10]; Japanese Cybersecurity Strategic Headquarters, 2020[11]). However, sectoral regulators take such guidance into account as part of their overall mandate to supervise operators in their sector.

Overall, governments share common objectives with respect to the types of measures that operators should take, such as adopting enhanced digital security risk management and sharing risk-related and/or best practice information, and/or reporting incidents.

As it is not possible to protect everything at the same level, the designated operators of critical activities need to identify the functions without which they could not effectively carry out their critical activities, as well as the critical parts of the digital ecosystem supporting these critical functions. Digital ecosystems includes hardware, software, networks and data, operational technologies that detect or cause changes in physical processes (such as industrial control systems), as well as the internal and external entities, persons, and processes that design, maintain and operate them, and the relationships between them. Lastly, operators need to systematically and cyclically manage digital security risk related to these critical functions. They conduct a digital security risk assessment of these critical functions, taking into account the digital ecosystem, and make a business decision to treat digital security risk.

A key challenge for government intervention is to formulate recommendations or requirements to implement state-of-the art digital security risk management at the appropriate level of detail. Digital technologies are extremely dynamic, and so are threats, vulnerabilities, as well as techniques and processes to protect digital ecosystems. If policy measures are too detailed, public policies aiming to incentivise operators to take more robust security measures may be quickly outdated and become an inhibiting factor for operators, without providing the expected level of security. If they are too generic, operators may face regulatory uncertainty if they experience difficulties in interpreting policies for implementation and compliance purposes.

In the United States, for example, the government promotes the Cybersecurity Framework developed by the National Institute of Standards and Technologies (NIST) in co-operation with the industry (NIST, 2018[12]). The Cybersecurity Framework is voluntary guidance based on existing standards, guidelines, and practices. This Framework is widely recognised as a useful tool, including beyond the United States and beyond operators of critical activities.

In Japan, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) provides guidance through the Cybersecurity Policy for

Critical Infrastructure Protection which includes Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure, as well as Risk Assessment Guide for Operators (Japanese Cybersecurity Strategic Headquarters, 2020[11]; Japanese Cybersecurity Strategic Headquarters, 2019[13]; Japanese Cybersecurity Strategic Headquarters, 2019[14]).

In March 2021, the Korea Internet & Security Agency (KISA) issued "Technical Vulnerability Analysis and Assessment Guidelines for Critical Information Infrastructure" in order to strengthen the cybersecurity capacity of critical infrastructure operators.

The European Union's NIS Directive is transposed in different ways across countries. In France, the compliance requirements are quite detailed and include, for example, the data that the operator needs to gather when mapping its critical information systems (JORF, 2018[1]; ANSSI, 2021[2]). In the United Kingdom the requirements stated in the law are quite high-level and complemented by guidance from the National Cyber Security Centre (NCSC) ("Cyber Assessment Framework") (NCSC, 2019[17]; HMSO, 2018[18]). In both cases however, non-compliance with the regulation can lead to financial penalties. The NIS Coordination Group, established by the NIS Directive, provides high-level guidance for EU members on what measures they can require operators to take (NIS Cooperation Group, 2018[19]).

The 2019 OECD Recommendation on digital security of critical activities represents the consensus among OECD members regarding the high-level set of risk management measures that operators should be recommended to adopt (OECD, 2019[4]).

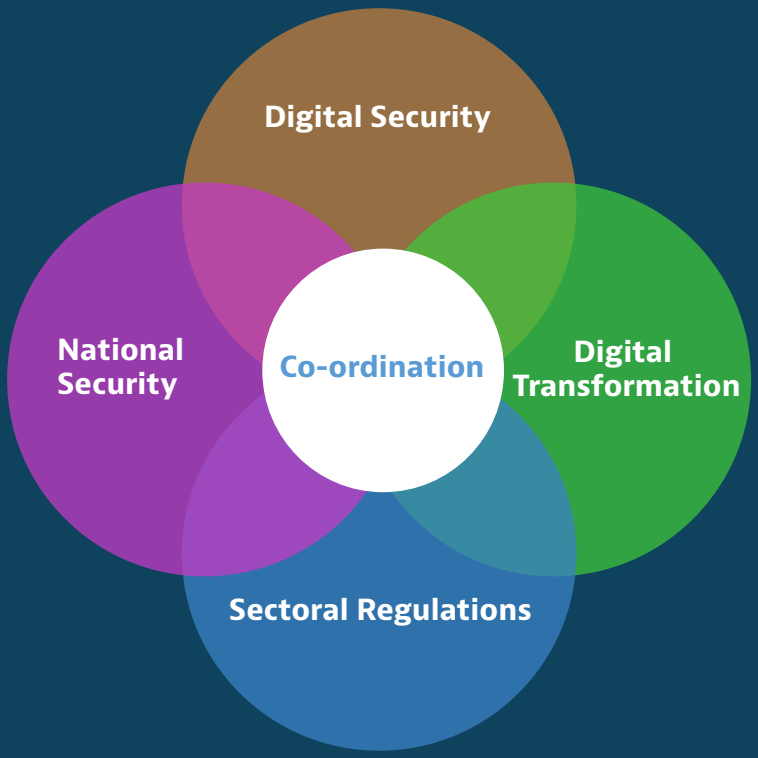
In the European Union, the NIS Directive also establishes an obligation for operators to notify significant digital security incidents to the competent national authority and to notify cross-border impact. This requirement is different from but complementary with the requirement established by the EU General Data Protection Regulation for the notification of personal data breaches (European Commission, 2021[3]). Incident notification, which in some non-EU countries can be voluntary, allows the government to have a better situational awareness and appropriately adjust possible assistance.

Governance and capacity

Policies to enhance the digital security of critical activities are at the crossroad of several areas (Figure 1). They aim to support digital transformation by ensuring trust in activities that are essential to the functioning and prosperity of our economies and societies. Therefore they are part of a national *digital transformation policy* agenda, as well as national *digital security* agenda. As explained above, policies to enhance the digital security of critical activities can build upon the national risk assessment resulting from the country's critical infrastructure protection framework, which is often part of a *national security*

and public safety agenda. In addition, they also span across different sectors such as finance, energy, communications, transports and health care, with specific technical, market, economic, regulatory, cultural and other characteristics. Therefore, these policies can also be viewed as part of several *sectoral* agendas (e.g. smart cities, smart grid, smart health, etc.) and have to take into account sectoral regulations and market conditions.

Figure 1. Co-ordination to enhance the digital security of critical activities



Source: Author.

It is generally a significant challenge for governments to take into account these different perspectives in a balanced manner. Three elements are required: 1) adopting at the highest level of government, and as part of a national digital security strategy, clear objectives to strengthen digital security and resilience of critical activities, 2) adopting a domestic governance mechanism that allocates responsibility to one or more government bodies to enhance the digital security of critical activities within and across sectors, and 3) ensuring a whole-of-government domestic co-ordination to establish intra-governmental co-operation, ensure consistency of the measures adopted across sectors, allocate resources across responsible government bodies and create a critical mass of expertise and skills, and facilitate cross-border co-operation.

There is no one-size-fits-all approach to a whole-of-government co-ordination in OECD countries. Governance frameworks vary significantly, according in part to a country's constitution, style of government, and administrative structure. In all cases, governance frameworks need to ensure consistency with human rights and fundamental values.

The governance relates generally to three key functions: 1*)* the definition of the overarching policy framework or strategy, 2*)* the implementation of the framework in each sector and 3*)* the operational capacity. The three functions can be centralised in a single body as in France (the National Agency for the Security of Information Systems, ANSSI), or distributed in different ways.

For example, the strategy development can be led by a department or ministry (e.g. Germany, UK, Japan), the operational capacity can be located in a separate agency (e.g. NCSC in the UK, the Federal Office for Information Security (BSI) in Germany, NISC in Japan), and the implementation of the framework and supervision can be centralised or decentralised through sectoral regulators (Box 4). In Denmark, the overarching policy framework was developed by the Ministry of Finance as part of the national digital security strategy, but each ministry responsible for a critical sector (energy, healthcare, transports, etc.) is required to develop a specific sub-strategy in its area of competence (Danish Ministry of Finance, 2018[21]). In many countries, the body in charge of operational digital security assistance can liaise with law enforcement and intelligence bodies.

Each approach has pros and cons. For example, a centralised approach facilitates regulatory consistency but makes detailed sector-specific regulation more difficult, requiring the central body to consult relevant sectoral regulators and create links with private operators of critical activities. A decentralised approach facilitates the development and implementation of sector-specific regulation while requiring more efforts to ensure consistency across sectors and provide the government with a holistic understanding of the situation. A key advantage of the decentralised approach is that sectoral regulators already have relationships with operators in their sectors and understand their constraints. However, operators may be reluctant to disclose digital security-related information to sectoral regulators which might be used for other regulatory purposes (European Commission, 2019[22]).

An important aspect is the need to ensure that the responsible body (or bodies) has (or have) sufficient capacity to accomplish its (their) tasks, including funding and resources as well as digital security expertise, which is scarce in most countries and difficult to retain in the public sector. It may seem easier to aggregate a critical mass of digital security expertise through a central body, as the bulk of technical digital security challenges is common to all sectors.

Box 4. Governance models

Canada follows a centralised model. The Department of Public Safety and Emergency Preparedness (Public Safety Canada) supports operators of critical activities to better secure their information systems. Operational capacity, previously distributed across different departments and agencies has been unified in a single Canadian Centre for Cyber Security ("Cyber Centre") (Public Safety Canada, 2020[23]).

Japan follows a decentralised approach where sectoral regulators, as part of their general mandate, supervise the digital security of critical operators in their sector. However, NISC co-ordinates the overarching policy, and provides guidance to operators and sectoral regulators. NISC is a central body reporting to the Cabinet of the Prime Minister.

In the United States, policy to enhance the digital security of critical activities is led by the Department of Homeland Security (DHS) and in particular DHS' Cybersecurity and Infrastructure Security Agency (CISA).

In the European Union (EU), the NIS Directive required EU member states to designate one or more competent authority or authorities to supervise this area. Sixteen EU members have designated a single body including Czech Republic, Estonia, France, Germany, Greece, Hungary, Ireland, Italy, Lithuania, Portugal, Slovakia, Slovenia, and Spain. Ten EU countries have designated multiple bodies, including Austria, Belgium, Denmark, Finland, Latvia, Netherlands, Poland, and Sweden. The United Kingdom also falls in this category (European Commission, 2020[24]; KPMG, 2019[25]).

Sources: (Public Safety Canada, 2020[23]); (European Commission, 2020[24]; KPMG, 2019[25]).

Governments can address this issue by separating the policy from the operational expertise. For example, in the United Kingdom, the NCSC supports sectoral regulators by offering technical advice and Computer Security Incident Response Team (CSIRT) services. A central body can also issue guidance and guidelines to help sectoral agencies carry out their mission, as in Japan and the UK (Japanese Cybersecurity Strategic Headquarters, 2020[11]; Department for Digital, Culture, Media & Sport, 2018[26]). In reality, most countries follow a relatively hybrid model. Countries with a centralised approach compensate centralisation through intra-governmental consultations and co-operation, and countries with a decentralised model generally maintain a central operational body to support sectoral regulators and ensure holistic situational awareness.

As part of this overarching framework, governments should build capacity to support digital security risk management and resilience of critical activities. This includes developing a new or strengthening an existing incident response capability through a computer security incident response team (CERTs/CSIRTs)

or Security Operation Centre (SOCs), or several of them operating for example by sector. While governments need to have at least one CERT/CSIRT to address incidents in their own systems, other CERTs/CSIRTs are not necessarily public sector bodies. Governments also often take a leadership role to organise sector and cross-sector cybersecurity exercises or drills with operators to test and improve existing measures, including information flows between stakeholders during crises. Such exercises can involve partners across borders at regional (e.g. Cyber Europe organised by ENISA) and international levels (e.g. US-led Cyberstorm organised by CISA) (ENISA, 2020[4]; CISA, 2021[5]).

Trust-based partnerships

The development and implementation of policies to enhance critical activities requires a multistakeholder approach involving government, business, civil society and the technical community.

The multiplicity and complexity of digital dependencies across sectors and borders and along critical activities' value chains create a shared digital security risk that no single actor can significantly reduce for the benefit of all. Each actor is therefore dependent upon and responsible towards all others to manage digital security risk. The establishment of sustainable public-public, public-private and private-private partnerships across sectors and borders, is an essential tool to ensure that digital security risk management of critical activities appropriately takes account of such dependencies. Such partnerships enable participants to share risk-related information (e.g. threats, vulnerabilities, incidents, and impact), as well as experience and good practice on digital security risk management. They can also help improve public policies over time. However, such partnerships cannot emerge without establishing a sufficient level of trust among stakeholders.

There is no one-size-fits all approach to build and structure such partnerships. They can leverage existing bodies such as sectoral Information Sharing and Analysis Centres (ISACs) and CERTs/CSIRTs which may be national (e.g. ICARO in Spain, the network of CSIRTs in Portugal, the Forum for Information Exchange in Lithuania, CERT.LU in Luxemburg, the National Cyber Security Centre (NCSC) in Norway, home of the Norwegian CERT (NorCERT), the National Coordinating Center for Communications (NCC) and Aviation Information Sharing and Analysis Center in the United States, etc.), regional (e.g. EU FI-ISAC and EE-ISAC in the financial and energy sectors), or international (e.g. FS-ISAC in the financial sector) (ENISA, 2018[29]).

Partnership can also be more holistic. For example, the German government established a public-private partnership (UP KRITIS) with operators of critical activities when designing the country's critical infrastructure protection plan in 2005 (UP KRITIS, 2014[30]). In the UK, the Cyber Security Information Sharing Partnership (CiSP) is a joint industry and government initiative run by the NCSC

to allow organisations to share cyber threat information in a secure and confidential environment (NCSC, 2021[6]). In Japan, information sharing takes place through 19 sectoral CEPTOARs (i.e. Capability for Engineering of Protection, Technical Operation, Analysis and Response) and through a cross-sector CEPTOAR Council (NISC, 2020[32]). In the United States, CISA maintains a Cyber Information Sharing and Collaboration Program (CISCP) to enable actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure (CI) sectors (CISA, 2021[7]). The Korea Internet & Security Agency (KISA) has been running a public-private cyber threat intelligence sharing programme called Cyber Threat Analysis & Sharing (C-TAS). C-TAS is a membership-based co-operation programme, where members share their cyber threat information in order for them to facilitate cyber threat prevention and handling at an early stage. As of March 2021, the programme gathered 306 domestic organisations, including operators of critical information infrastructures.

Considering the sensitivity of the information to be exchanged, partnerships require trust. Many stakeholders often do not trust governments on digital security issues (OECD, 2021[34]; OECD, 2021[35]). The *OECD 2019 Recommendation on digital security of critical activities* provides a general list of conditions to establish trust with a view to enabling sustainable public-public, public-private and private-private partnerships. These conditions include the need for clear aims, values and rules, mutual benefits over time, respect for privacy and personal data protection regulation as well as other regulation protecting the confidentiality of information such as trade secrets. In particular, it is important that partners ensure that the information they receive from other partners will only be used for defensive purposes and is managed in a manner consistent with regulations protecting personal data and other information such as trade secrets (OECD, 2019[4]).

Annex: A selection of policy approaches to enhance the digital security of critical activities

Key policy or regulation

EU Directive on security of network and information systems (NIS Directive)

Responsible entity: European Commission

Description: The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU. It was adopted and entered into force in 2016. EU Member States had to transpose the Directive into their national laws by 9 May 2018 and identify operators of essential services by 9 November 2018. Members have to ensure 1*)* preparedness by being appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority, 2*)* co-operation among all the Member States, by setting up a Cooperation Group and a CSIRT Network, 2*)* a culture of security across sectors which are vital for the economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in sectors identified by the Member States as operators of essential services have to take appropriate security measures and to notify serious incidents to the relevant national authority. Key digital service providers (search engines, cloud computing services and online marketplaces) have to comply with the security and notification requirements under the new Directive.

Read more: *https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive.*

Japan's Cybersecurity Policy for Critical Infrastructure Protection (CIP)

Responsible entity: Japan's National Center of Incident readiness and Strategy for Cybersecurity (NISC)

Description: The 4th edition of the Cybersecurity Policy for CIP aims to promote activities for reduction of risk of outage to Critical Infrastructure Services (CISs) resulting from cyberattacks, natural disasters, etc. and ensuring resilience in order to provide CISs safely and continuously, based on active involvement of top management (Mission Assurance). The policy focuses on the maintenance and promotion of safety principles, the enhancement of the information sharing system and incident response capacity, as well as the promotion of risk management and preparation of incident. The policy

promotes critical infrastructure protection through public-private partnerships within and across 14 sectors. The governance involves 5 ministries in charge of these sectors as well as ministries and agencies with a role on cybersecurity, ministries in charge of crisis management, ministries in charge of disaster prevention, and operators involved in cyberspace (e.g. vendors).

Read more: *www.nisc.go.jp/eng/#sec4.*

Brazil's Cybersecurity Framework

Responsible entities: Institutional Security Cabinet of the Presidency of the Republic of Brazil (GSI/PR) for the National Critical Infrastructure Security Strategy, National Cybersecurity Strategy and Federal Cyber Incident Management Network.

Brazil's National Telecommunications Agency (Anatel) for the cybersecurity regulation for the telecommunications sector.

Description: Brazil's National Critical Infrastructure Security Strategy approved in December 2020 defines strategic objectives and initiatives related to 4 essential pillars: institutional co-ordination; awareness and capacity building; data and information management; and the promotion of co-ordinated actions. In addition, Brazil's National Cybersecurity Strategy approved in February 2020 defines 3 strategic objectives guiding 10 strategic actions. The objectives are: 1) making Brazil more prosperous and reliable in the digital environment; 2) increasing Brazilian resilience to cyber threats; and 3) strengthening the role of Brazil in cybersecurity at the international level. These strategic objectives represent basic guidelines for the public and private sectors and for society to enjoy a resilient, reliable, inclusive, and secure cyberspace. At the sectoral level, the National Telecommunications Agency (Anatel) approved a cybersecurity regulation for the telecommunications sector in December 2020 which establishes mandatory provisions related to telecommunication critical infrastructure. Lastly, the Federal Cyber Incident Management Network, informally operational since 2006, was formally established in July 2021 to improve and maintain co-ordination in the federal public administration. It focuses on the prevention, treatment, and response to cyber incidents, in order to raise the level of cyber security resilience of information assets. It aims to disseminate measures to prevent, treat and respond to cyber incidents; share alerts on cyber threats and vulnerabilities; disclose information about cyber attacks; promote co-operation among Network participants and swift response to cyber incidents.

Read more:
www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm,
https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740,

www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm, www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm.

Measures for operators of critical activities

EU NIS Cooperation group's Reference document on security measures for Operators of Essential Services

Responsible entity: European Union's NIS Cooperation group

Description: The NIS Cooperation Group facilitates strategic co-operation between EU Member States regarding the security of network and information systems, including by publishing non-binding guidelines to the EU Members States. The Reference document on security measures for operators of essential services is based on information exchanges between Members. It provides high-level guidance for EU members on what measures they can require operators to take. It includes a set of principles and a list of domains of cybersecurity measures (governance, protection, defence, resilience).

Read more: *https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.*

US NIST Cybersecurity Framework

Responsible entity: US National Institute for Standards and Technology (NIST)

Description: In 2013, NIST was tasked with the development of a framework for reducing risk to critical infrastructure, and the Department of Homeland Security (DHS) with helping critical infrastructure use and understand this framework. The framework was expected to be used by critical infrastructure sectors and organisations to reduce and manage their cyber risk regardless of size or cybersecurity sophistication. The Framework is voluntary guidance, based on existing standards, guidelines, and practices. It can be used to align cybersecurity decisions to mission objectives; organize security requirements originating from legislation, regulation, policy, and industry best practices; communicate cybersecurity requirements with stakeholders, including partners and suppliers; integrate privacy and civil liberties risk management into cybersecurity activities; measure current state and express desired state; prioritize cybersecurity resources and activities; and analyse trade-offs between expenditure and risk.

Read more: *www.nist.gov/cyberframework.*

UK Cyber Assessment Framework

Responsible entity: UK National Cyber Security Centre (NCSC)

Description: The Cyber Assessment Framework (CAF) provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible. It is intended to be used either by the responsible organisation itself (self-assessment) or by an independent external entity, possibly a regulator or a suitably qualified organisation acting on behalf of a regulator. The NCSC cyber security and resilience principles provide the foundations of the CAF. The 14 principles are written in terms of outcomes, i.e. specification of what needs to be achieved rather than a checklist of what needs to be done. The CAF adds additional levels of detail to the top-level principles, including a collection of structured sets of Indicators of Good Practice.

Read more: *www.ncsc.gov.uk/collection/caf/nis-introduction.*

Japan Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure

Responsible entity: Cybersecurity Strategic Headquarters, Government of Japan

Description: This guideline contains cybersecurity measures, including high-priority and/or advanced items which should serve as a reference for all critical infrastructure sectors in order to contribute to preparation and revision of "safety principles". This guideline sets out items for information security measures in accordance with the Plan-Do-Check-Act (PDCA) cycle, to enable easy referencing for critical infrastructure operators when they are engaged in voluntary initiatives or continual improvements.

Read more: *www.nisc.go.jp/eng/pdf/principles_ci_ng_v5_r1.pdf.*

Korea Technical Vulnerability Analysis and Assessment Guidelines for Critical Information Infrastructures

Responsible entity: Korea Internet & Security Agency (KISA)

Description: In March 2021, the Korea Internet & Security Agency (KISA) issued "Technical Vulnerability Analysis and Assessment Guidelines for Critical Information Infrastructures" in order to strengthen critical infrastructure operators' cybersecurity capacity.

Read more:
www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=6&mode=view&p_No=259&b_No=259&d_No=106&ST=T&SV=.

Trust-Based Partnerships

Germany's UP KRITIS partnership

Responsible entity: German Federal Office for Information Security (BSI) and Federal Office of Civil Protection and Disaster Assistance (BBK)

Description: On a strategic and on an operative level, the German Federal Government follows a holistic approach to critical infrastructure protection, with the framework that served to prepare the German CIP Implementation Plan ("Umsetzungsplan KRITIS") in 2005-2006 in co-operation with critical infrastructure operators. The plan's publication in 2007 institutionalised the public-private co-operation "UP KRITIS", which aims to improve the protection of critical infrastructure across sectors. The increasing ICT security related risk has taken a greater part in UP KRITIS over time; however, UP KRITIS also deals with topics beyond IT in order to maintain and strengthen critical infrastructure availability and robustness. Comprehensive protection of critical infrastructure requires joint development and implementation of physical protection and IT security. The cross-sectoral co-operation between industry and the state within UP KRITIS has become a success, with over 750 organisations co-operating on the basis of mutual trust, exchanging ideas and experiences and learning from each other about critical infrastructure protection. All parties are thus finding better solutions, developing concepts, establishing contacts, holding exercises and developing a joint approach for cyber crisis management, within sectoral and thematic working groups. Furthermore, such working groups provide feedback on cyber security legislation.

Read more: *www.upkritis.de* and *www.kritis.bund.de/SubSites/Kritis/EN/activities/national/cipimplementationplan/cipimplementationplan_node.html*.

UK's Cyber Security Information Sharing Partnership (CiSP)

Responsible entity: UK National Cyber Security Centre (NCSC)

Description: The Cyber Security Information Sharing Partnership (CiSP) is a joint industry and government initiative set up to allow UK organisations to share cyber threat information in a secure and confidential environment. Members can benefit from engagement with industry and government counterparts in a secure environment, early warning of cyber threats, the ability to learn from experiences, mistakes, successes of other users and seek advice, an improved ability to protect their company network, and access to free network monitoring reports tailored to your organisations' requirements.

Read more: *https://www.ncsc.gov.uk/section/keep-up-to-date/cisp*.

United States' Cyber Information Sharing and Collaboration Program (CISCP)

Responsible entity: US Cybersecurity and Infrastructure Security Agency (CISA)

Description: The US Department of Homeland Security (DHS) Cyber Information Sharing and Collaboration Program (CISCP) enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure sectors. CISCP fosters this collaboration by leveraging the depth and breadth of DHS cybersecurity capabilities within a focused operational context. Through analyst-to-analyst sharing of threat and vulnerability information, CISCP helps partners manage cybersecurity risks and enhances our collective ability to proactively detect, prevent, mitigate, respond to, and recover from cybersecurity incidents. CISCP's overall objective is to build cybersecurity resiliency and to harden the defenses of the United States and its strategic partners. CISCP membership provides access to DHS analysts, and to a broad suite of DHS National Cybersecurity and Communications Integration Center (NCCIC) services and CISCP products. These DHS resources help reduce the cyberspace attack surface of the United States and its strategic partners and support cybersecurity information exchange.

Read more: *www.cisa.gov/ciscp.*

Japan's CEPTOAR

Responsible entity: Japan's NISC

Description: Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR) are organisations responsible for information sharing and analysis functions and relevant functions for critical infrastructure operators in Japan. They aim to facilitate proactive prevention of critical infrastructure outages as well as prevention of the spread of damage, prompt recovery, and prevention of recurring outage. CEPTOARs provide information from the Government to critical infrastructure operators and share information with stakeholders. CEPTOARs aim at activities that contribute to the improvement of the service maintenance and recovery capability of each critical infrastructure operator. 19 CEPTOARs are operating in 14 sectors. A CEPTOAR Council facilitates information sharing between CEPTOARs. It is an independent meeting structure that is not positioned under any other organizations including government organizations consisting of representatives from each critical infrastructure sector.

Read more: *www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4_summary_r1.pdf.*

Korea's C-TAS

Responsible entity: KISA

Description: KISA has been running a public-private partnership to facilitate the sharing of cyber threat intelligence called Cyber Threat Analysis & Sharing (C-TAS). As of March 2021, 306 domestic organisations, including operators of critical information infrastructures are members of C-TAS and share their cyber threat information to better prevent and handle cyber threats at an early stage.

Read more: *www.krcert.or.kr/webprotect/ctas.do.*

References

ANSSI (2021), *NIS : un dispositif de cybersécurité pour les Opérateurs de services essentiels*, https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/nis-un-dispositif-de-cybersecurite-pour-les-operateurs-de-service-essentiel/ (accessed on 3 September 2021). [16]

CISA (2021), *National Critical Functions*, https://www.cisa.gov/national-critical-functions (accessed on 3 September 2021). [5]

CISA (2021), *Cyber Information Sharing and Collaboration Program (CISCP)*, https://www.cisa.gov/ciscp (accessed on 3 September 2021). [33]

CISA (2021), *Cyber Storm: Securing Cyber Space*, https://www.cisa.gov/cyber-storm-securing-cyber-space (accessed on 3 September 2021). [28]

Danish Ministry of Finance (2018), *Danish Cyber and Information Security Strategy*, https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf. [21]

Department for Digital, Culture, Media & Sport (2018), *NIS Regulations: Guidance for Competent Authorities*, https://www.gov.uk/government/publications/nis-regulations-guidance-for-competent-authorities (accessed on 3 September 2021). [26]

ENISA (2020), *Cyber Europe*, https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme (accessed on 3 September 2021). [27]

ENISA (2018), *Information Sharing and Analysis Center (ISACs) - Cooperative models*, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models (accessed on 3 September 2021). [29]

European Commission (2020), *Proposal for directive on measures for high common level of cybersecurity across the Union*, https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union (accessed on 3 September 2021). [8]

European Commission (2020), *State-of-play of the transposition of the NIS Directive*, https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive (accessed on 3 September 2021). [24]

European Commission (2019), *Report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services*, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52019DC0546&from=EN. [9]

European Commission (2019), *Report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of the NIS Directive*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546. [22]

European Commission (2021), *What is a data breach and what do we have to do in case of a data breach?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en (accessed on 3 September 2021). [20]

European Union (2016), *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG. [6]

Government of Japan (2018), *Cybersecurity Strategy*, https://www.nisc.go.jp/eng/pdf/cs-strategy2018-en-booklet.pdf. [10]

HMSO (2018), *The Network and Information Systems Regulations 2018*, https://www.legislation.gov.uk/uksi/2018/506/contents/made (accessed on 3 September 2021). [18]

Japanese Cybersecurity Strategic Headquarters (2020), *The CybersecurityPolicy for Critical Infrastructure Protection (4th Edition)*, https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4_r2.pdf. [11]

Japanese Cybersecurity Strategic Headquarters (2019), *Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure(5th Edition)*, https://www.nisc.go.jp/eng/pdf/principles_ci_eng_v5_r1.pdf. [14]

Japanese Cybersecurity Strategic Headquarters (2019), *Risk Assessment Guide Based on the Concept of Mission Assurance in Critical Infrastructure (1st edition)_r1*, https://www.nisc.go.jp/eng/pdf/guide_ci_eng_r1.zip. [13]

JORF (2018), *Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'art. 10 du décret n° 2018-384 du 23 mai 2018*, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037444012/ (accessed on 3 September 2021). [15]

KPMG (2019), *Complying with the European NIS Directive. Cybersecurity for critical infrastructures*, https://assets.kpmg/content/dam/kpmg/fr/pdf/2019/04/fr-complying-with-the-eu-nis-directive.pdf. [25]

NCSC (2019), *NCSC CAF guidance*, https://www.ncsc.gov.uk/collection/caf (accessed on 3 September 2021). [17]

NCSC (2021), *CiSP*, https://www.ncsc.gov.uk/section/keep-up-to-date/cisp (accessed on 3 September 2021). [31]

NIS Cooperation Group (2018), *CG Publication 01/2018 - Reference document on security measures for Operators of Essential Services*, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643. [19]

NISC (2020), *Summary of the Cybersecurity Policy for CIP (4thEdition)*, https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4_summary_r1.pdf. [32]

NIST (2018), *Cybersecurity Framework*, https://www.nist.gov/cyberframework (accessed on 3 September 2021). [12]

OECD (2021), *Encouraging vulnerability treatment: How policy makers can help address digital security vulnerabilities*, OECD, Paris, http://www.oecd.org/digital/encouraging-vulnerability-treatment.pdf. [35]

OECD (2021), "Encouraging vulnerability treatment: Overview for policy makers", *OECD Digital Economy Papers*, No. 307, OECD Publishing, Paris, https://dx.doi.org/10.1787/0e2615ba-en. [34]

OECD (2020), "Going Digital integrated policy framework", *OECD Digital Economy Papers*, No. 292, OECD Publishing, Paris, https://dx.doi.org/10.1787/dc930adc-en. [2]

OECD (2019), "Policies for the protection of critical information infrastructure: Ten years later", *OECD Digital Economy Papers*, No. 275, OECD Publishing, Paris, https://dx.doi.org/10.1787/efb55c54-en. [3]

OECD (2019), *Recommendation of the Council on Digital Security of Critical Activities*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456. [4]

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264245471-en. [7]

Public Safety Canada (2020), *National Cyber Security Action Plan (2019-2024)*, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx#a04 (accessed on 3 September 2021). [23]

UP KRITIS (2014), *UP KRITIS Public-Private Partnership for Critical Infrastructure Protection. Basis and Goals*, https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/UP_KRITIS.pdf?__blob=publicationFile. [30]