OECD publishing

POLICIES FOR THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE

TEN YEARS LATER

OECD DIGITAL ECONOMY POLICY PAPERS

February 2019 **No. 275**

OECD
BETTER POLICIES FOR BETTER LIVES

This paper was approved and declassified by the Committee on Digital Economy Policy on 16 November 2018 and prepared for publication by the OECD Secretariat.

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

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

#GoingDigital

Note to Delegations:
This document is also available on O.N.E under the reference code:
DSTI/CDEP/SPDE(2017)14/FINAL

Foreword

After the adoption of the 2002 *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* ("Security Guidelines"), OECD work on digital security focused on their implementation with respect to the protection of critical infrastructures. A comparative analysis of national policy in seven volunteer countries was carried out. Its findings led to the development and adoption, in 2008, of the *Recommendation of the Council on the Protection of Critical Information Infrastructure* (CIIP Recommendation). The CIIP Recommendation was to be reviewed by the Committee on Digital Economy Policy[1] (CDEP) every five years. In 2012, CDEP agreed to postpone the first review until after completion of the revisions to the 2002 Security Guidelines, which were replaced in 2015 with the *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity* ("Security Risk Recommendation").

In 2016, the Working Party on Security and Privacy in the Digital Economy (SPDE) initiated the review process of the CIIP Recommendation by circulating a questionnaire to delegations. To further inform the review, a roundtable on the "Future of the protection of critical information infrastructures" was organised at the 41st SPDE meeting in May 2017. A first draft summary of responses was discussed at the 42nd SPDE meeting in October 2017. Discussions related to this subject area also took place at the Going Digital Workshop on Digital Security and Resilience in Critical Infrastructure and Essential Services on 15-16 February 2018.

This paper consolidates these elements to provide an analysis of policies for the protection of critical information infrastructures across OECD countries that will guide the updating of the 2008 CIIP Recommendation.

It was drafted by Laurent Bernat and Suguru Iwaya with contribution from Elettra Ronchi from the OECD Secretariat, as well as Nick Mansfield and Benjamin Dean, consultants to the OECD.

Table of contents

EXECUTIVE SUMMARY

The Working Party on Security and Privacy in the Digital Economy (SPDE) has undertaken a two year process to review and possibly update the *Recommendation of the Council on the Protection of Critical Information Infrastructure* (CIIP Recommendation) ten years after its adoption. A questionnaire was circulated amongst OECD members and participants in the Committee on Digital Economy Policy to collect input for the review. Eighteen countries responded to the questionnaire, representing a variety of regions, country cultures, sizes, and digital maturity. This document provides an analysis of these responses and suggestions to guide the updating of the Recommendation. The update of the Recommendation serves as an opportunity to make changes to its purpose and scope; to insert key messages based on overarching themes from the responses; and to adjust the Recommendation in line with current and anticipated evolutions in contexts, risks and policies.

The update comes against a backdrop of fast digital transformation and increased digital reliance of businesses and governments; increased frequency and severity of attacks on CII; the rise of state-sponsored attacks including digital sabotage and espionage; and the increased capacity of attackers. As a result, there is a pressing need to collect and share common good practices in order to assist policymakers tasked with managing the risks associated with these emerging trends, drivers and challenges.

The concept of "Critical Information Infrastructure" (CII) was initially introduced at the international level to raise awareness on the need to develop policies in this then emerging area. However, although well recognised by subject matter experts, it has been rarely used to develop domestic policy frameworks. The inherent complexity of the concept has become a source of confusion rather than inspiration. An updated Recommendation no longer needs to use the concept of CII. It should instead focus on the application of the Principles of the 2015 *Recommendation of the Council on digital security risk management for economic and social prosperity* ("Security Recommendation") to the protection of essential services, activities, or functions.

Countries that developed a CIIP policy framework a decade ago often follow a risk management approach that focuses on protection of information infrastructure. Those with a more recent framework generally follow a "service approach", which primarily focuses on the risk to services, functions or activities that are critical to the economy and society rather than on risk to the information infrastructure assets that support these services. The emergence of a "service approach" resembles the paradigmatic transition that occurred between the 2002 Security Guidelines and the 2015 Security Recommendation. To ensure alignment with the 2015 Security Recommendation, the updated Recommendation should focus on the protection of essential services against digital security risk rather than the protection of critical information infrastructures.

Policies related to digital security risk to essential services tend to be grounded in both digital security strategies and national risk management frameworks, also known as critical infrastructure protection frameworks. This is partly the consequence of widespread adoption of a whole-of-government approach in setting policies for the protection of essential services against digital security risk across countries. The scope of the updated Recommendation would need to reflect these two policy areas. Moreover, to account for the differing levels of maturity across countries, the updated Recommendation could

suggest a sequential process for building a policy framework to enhance digital security of essential services. This would emphasise the need for gradual change based on the progressive accumulation of experience and expertise rather than attempting to implement all potential policies at once.

Although responses revealed many commonalities with respect to the high-level objectives and content of CIIP policies, a number of differences across countries became evident. These differences are generally related to how policies are implemented. For example, most respondents agree on the need for a whole-of-government approach, but adopt varying degrees of governance centralisation and decentralisation. Similarly, they support increased efforts on the part of operators, but regulatory intensity varies from mandatory to voluntary measures. These differences reflect cultures and styles of government rather than fundamental discrepancies in approaches. An updated Recommendation would need to build upon the many commonalities, and accommodate these differences, in part by focusing on policy content, and leaving flexibility with regards to policy implementation.

One of these commonalities was co-operation, which is fundamental to effective frameworks and policies to protect essential services given the multiplicity of dimensions to contend with (e.g. economic, social, national security, technical, legal, etc.) and dependencies to manage (e.g. digital dependencies, dependencies across actors, sectors and borders). No single stakeholder (e.g. government, operator) can address the challenges associated with CIIP alone as each has differing authority and capacity to act in terms of resources and expertise. The updated Recommendation could articulate a strong high-level policy message around the theme of co-operation and provide examples of how such co-operation could be implemented, such as through partnerships. It could also provide guidance on the trust to be established to facilitate such partnerships.

Reinforcing the need for co-operation, managing various forms of dependencies and interdependencies emerged as an important but inadequately understood concept across respondents, particularly with relation to cross-border dependencies. Two dimensions of "digital dependencies" could be reflected in the updated Recommendation. The first builds on the type of failure: common cause failure; digital propagation failure; and cascade failure. The second relates to cross-border dependencies, which are the consequence of the globally interconnected nature of digital technologies. Particularly with relation to this latter dimension, the updated Recommendation could provide greater detail at a high level or more operational level regarding cross-border co-operation.

Across countries there remains little consistency in the way terms such as "essential", "critical", or "vital" and "services", "infrastructures", "activities" or "functions" are used. While all respondents' definition and understanding of critical infrastructure and CII were based on the severity of the consequences of disruption on an essential/critical part of the national economy or society, a broad range of criteria were used to define the severity of consequences. Although the updated Recommendation is unlikely to eliminate such terminological differences which are often related to existing national risk management frameworks, it can provide a common basis to facilitate domestic co-operation between governments and operators, and international co-operation among all stakeholders. A separate background or explanatory note to the Recommendation could usefully provide more details about terminology.

Introduction

This document provides a summary and analysis of the responses to a questionnaire circulated for the review of the 2008 Recommendation of the Council on the protection of critical information infrastructures ("CIIP Recommendation"). Eighteen countries responded to the questionnaire, representing a variety of regions, country cultures, sizes, and digital maturity[2]. Respondents are at different stages of policy maturity, ranging from countries with experience on a policy framework established ten years ago to countries in the process of developing their approach. Despite such differences, almost all respondents express support to update the 2008 Recommendation of the Council on the Protection of Critical Information Infrastructure ("CIIP Recommendation")[3]. As agreed by SPDE, responses received by the Secretariat are kept confidential and this report does not make explicit references to specific countries.

The document begins with the purposes for the update of the Recommendation. This is followed by suggestions for adjustments to the scope of the updated Recommendation. Key messages for the updated Recommendation are then provided and structured around four main overarching notions. Additional information from the responses to the questionnaire; an explanation of the concept of dependencies and interdependencies; responses from non-governmental stakeholders[4] to the questionnaire and the questionnaire itself can be found in a series of Annexes.

In addition to responses to the questionnaire, the analysis in this report also benefited from discussions at SPDE meetings in December 2016 and May 2017 (Roundtable on the Future of the Protection of Critical Information Infrastructures) as well as discussions at the 2018 Going Digital Workshop on Digital Security and Resilience in Critical Infrastructure and Essential Services.

1. Purposes of an Updated Recommendation

Ten years ago, CIIP was a new policy area and so one objective of the CIIP Recommendation was awareness raising. Today, the need for awareness has diminished. Instead, the need for clear messages about common good practice has now gained greater importance. An updated Recommendation would aim to serve several purposes including:

- Clarification of the scope of this policy area including where is stands within the broader picture of digital security and national risk management policy (often called critical infrastructure protection or CIP) as well as articulation of clear high-level messages to policy makers.
- An update to the core concepts so as to ensure coherence with the Recommendation's parent instrument, the 2015 *Recommendation of the Council on digital security risk management for economic and social prosperity* ("Security Risk Recommendation"), which replaced the 2002 *Guidelines on the Security of Information Systems and Networks* ("Security Guidelines").
- Recognition of changes in the digital environment (e.g. new technologies such as the IoT, artificial intelligence, big data; the sophistication and number of threats, etc.), the economy and society (e.g. the digital transformation and increased digital reliance of the economy and society), and public policies (e.g. national digital security strategies, existing CIIP and national risk management frameworks, emergence of national security in digital security policy, etc.). It would reflect the experience and lessons learned by those countries that adopted a framework ten years ago and the views of countries that have stepped into this area more recently.
- Updates to good practice, where appropriate, while recognising that many principles of the CIIP Recommendation are still relevant and should be preserved.

2. Scope of the updated Recommendation

2.1. The concept of CII is dated

The notion of CII was initially conceived over ten years ago to bring different domestic digital security policy approaches addressing critical infrastructures (OECD, 2007[1]) under a common and wide umbrella.[5] The CIIP Recommendation used this concept to, in turn, unite digital security policy experts focused on critical infrastructure protection under one single banner in order to raise awareness and bring policy coherence to this emerging area. While some countries do use it also at the domestic level, perhaps more as a label than as an operational concept, the analysis of the responses shows that the concept of "Critical Information Infrastructure" (CII) has been rarely used to develop domestic policy frameworks.

The concept of CII is characterised by its inherent complexity, which distinguishes it from other areas of national risk management. This gives the misleading impression that CIIP is a standalone policy area, akin to but somehow separate from national risk management. Instead, it should be considered an integral component thereof.

The concept of CII builds on the concept of "critical infrastructure", which is a relatively recent development. CII as a concept posits that interconnected information systems and networks sharing certain characteristics ("the disruption or destruction of which would have a serious impact…" etc.) form together a critical infrastructure akin to electricity, finance, transport and other critical infrastructures. In this sense, CII may be viewed as an evolution of the telecommunications critical infrastructure, which became entirely digital over the same period (Wenger, 2002, pp. 7-8[2]), and upon which other critical infrastructure rely. The CII concept also tends to focus on the technical assets (i.e. information systems and network) that support economic and social activities rather than on the activities themselves.

However, the concept of CII extends beyond the telecommunications sector. It includes the information systems and networks of the operators of other critical infrastructures such as energy, finance, and transport infrastructures. In contrast to other critical infrastructures, which are associated with a particular sector, CII covers not just a specific sector but also the important components scattered across all other critical sectors. Furthermore, the concept of CII implies that every operator of critical infrastructure (e.g. an electricity company, a bank) is also an operator of critical information infrastructure. This is because critical infrastructure operators also operate information systems and networks that are critical to their own functioning. At this point, the complexity of the concept of CII becomes evident, which helps to explain why it was and continues to be rarely used as a basis for public policy. Put simply, it is too difficult a concept to integrate within broader national risk management frameworks. Nevertheless, the concept may remain useful at the international level as a common umbrella term to bring together the relevant expert community (e.g. in fora such as (ENISA, 2015[3]), (GFCE Meridian, 2016[4])etc.).

The promotion of the CII concept was useful ten years ago to single out the digital security aspects of national risk management. Now that policy makers have become more aware of the importance of this area, the inherent complexity of that very concept has become a source of confusion rather than inspiration. An updated Recommendation no longer needs to use the concept of CII. Rather, it should focus on the application of the 2015 digital

security risk management principles to the protection of essential services. This would not necessarily mean that governments wishing to continue to use the CII concept or terms would not be aligned with the instrument. As noted above, CII was used in the 2008 Recommendation as a broad umbrella to characterise the area rather than as an operational policy concept.

2.2. The scope of the updated Recommendation should clearly be placed within the broader context of national risk management

Policies related to the digital security risk of essential services tend to be grounded in both digital security strategies and national risk management frameworks. For the Recommendation to remain relevant to policy makers, it is important to provide messages and guidance that are consistent with these two policy areas.

A suggestion might be to follow the risk assessment process, which is typically carried-out at three stages and levels, each of which has dependencies and interdependencies. They may provide helpful guidance in defining the scope of the Recommendation:

- *Stage 1:* A national risk assessment is carried out to identify essential services. This step generally requires criteria on 'criticality' to be set at the national level, which then leads to the identification of users and operators of essential services.
- *Stage 2:* Risk assessments are carried out to identify the components of each essential service that are critical to its delivery (i.e. without these components, the delivery of the essential service would not occur). Such components can include the specific business lines, functions, sites, plants, etc. within the operator that delivers the service. This step generally takes place at the operators' level and should be part of the operator's overarching enterprise risk management.
- *Stage 3:* A digital security risk assessment focusing on critical components identified in stage 2, which indicates the digital assets to be protected from failures related to integrity, availability and confidentiality. This step is the part of the operator's enterprise risk management that focuses on digital security (cf. 2015 Security Risk Recommendation).

These stages are part of an overall process that identifies what is critical within that which is deemed essential. The goal is to allocate greater attention and resources to the critical given the serious consequences of not doing so. The scope of the updated Recommendation would focus on stage 3, which would fit within the bigger picture of stages 1 and 2.

2.3. A focus on essential services rather than information infrastructures would align the updated Recommendation with its parent instrument

Countries that developed a CIIP policy framework a decade ago often follow a risk management approach focusing on information infrastructure. This is in line with the 2008 CIIP Recommendation and with its parent instrument, the 2002 Security Guidelines. Countries with a more recent framework generally follow a "service approach", whereby risk management focuses on services, functions or activities that are critical to the economy and society rather than on the information infrastructure assets that support these services.

The emergence of a "service approach" is reminiscent of the transition that occurred from the 2002 Security Guidelines to the 2015 Security Risk Recommendation. This transition saw the focus of digital security risk management shift from information systems and

networks (i.e. the information infrastructures or assets) to the economic and social activities (i.e. the services or functions) that rely on them.

In contrast to the activities or services-focused approach of the 2015 Recommendation, the technical assets-focused approach of the 2002 Security Guidelines does not lead to digital security risk assessments that take into account the full range of effects due to uncertainty[6] associated with delivery of a service. This is because the service itself is not directly part of the assessment. A technical risk management approach is likely to lead to:

- A technical rather than economic and social appreciation of risk appetite and acceptable level of residual risk.
- A risk assessment focusing on the information infrastructure as an end in of itself rather than as a means to deliver services.
- Business continuity and resilience measures that do not appropriately take into account the economic and social context of service delivery.
- Narrow recognition of just the responsibilities owned by organisations' information infrastructure leadership, which typically relate solely to the performance of the technical assets. This excludes organisations' economic and social (i.e. business) leadership, which are primarily responsible for the delivery of the actual service.
- A risk assessment that does not necessarily encompass the whole service's value chain beyond that which is deemed critical *information* infrastructures.
- A risk assessment that probably does not appropriately address data-related risk given that the value of data depends on the service they are related to rather than on the digital infrastructure which carries them (OECD, 2015[5])[7].

To ensure alignment with the 2015 Security Risk Recommendation, the updated Recommendation should focus on the protection of essential services against digital security risk rather than the protection of critical information infrastructures themselves.

2.4. Further discussions are needed on detailed terminology

There is little consistency in the way clusters of terms are used across countries. Common clusters include: "essential", "critical", and "vital" or "services", "infrastructures", "activities" and "functions". Some countries draw specific distinctions between terms such as "function" and "service", or "essential" and "critical" though these distinctions are not necessarily shared across countries. In many cases, the terminology used has been inherited from the broader national risk management framework.

As a result, the terminology to be used in the updated Recommendation remains unclear. Given this constraint, the updated Recommendation should not aim to prescribe a particular set of terms but rather provide a coherent semantic framework to understand how to approach this area. This approach should allow countries to then use or adapt certain terms when they develop their own domestic frameworks and policies. A separate background or explanatory note could usefully provide more details related to the issues associated with CIIP terminology as well as the terms themselves.

3. Main overarching themes

Four main overarching themes emerged from analysis of the responses to the questionnaire. These can be used as a means by which to articulate key messages for the updated Recommendation.

3.1. Dependencies and interdependencies are fundamental challenges

Most respondents underlined the importance of addressing dependencies and interdependencies for CIIP. However, parts of the questionnaire intended to identify policy aspects related to interdependencies proved inappropriate, probably because they were built on the concept of CII.

The 2008 CIIP Recommendation mentions dependencies and interdependencies. However, it does not explain what they are or how to take them into account. The dependency of all essential services upon digital assets (hardware, software, networks and data) justifies the need to integrate digital security risk in national risk management and makes co-operation across operators, public and private sectors and borders essential. Therefore, dependency should be a central concept in the updated Recommendation.

Two dimensions of "digital dependencies" could be reflected in the updated Recommendation. This is because they underlie essential policy principles such as the need for co-operation and co-ordination as well as integration within national risk management.

The first dimension is built on three specific types of failure that can be considered as characteristic of digital dependency:

1) *Common cause failure*: where a vulnerability that affects a digital component, on which several or all essential services depend, is subsequently exploited. This causes massive chaos and damages simultaneously across the economy.
2) *Digital propagation failure*: when a digital security threat to an operator of essential service successfully propagates to other operators, within the same and/or in different sectors, eventually causing damage to a large range of services, meeting the criteria of national criticality.
3) *Cascade failure*: when the disruption of the delivery of an essential service caused by a digital security incident cascades onto another essential service, subsequently causing disruption to its delivery.

Cross-border dependencies form the second dimension of "digital dependencies". They result from the globally interconnected nature of digital technologies, which results in dependencies across borders. They may arise in combination with the aforementioned dependencies that occur across services. The 2016 denial of service attack on Dyn demonstrated this kind of dependency as access to websites from Europe was affected by an incident taking place in the United States.

3.2. Co-operation and partnerships are fundamental to address the multiplicity of dimensions and dependencies

Co-operation emerged as a common theme that transcended all differences across respondent countries. Co-operation appears in the context of policy development and policy

implementation, both within and across sectors (public-public, public-private, private-private) and within and across borders (sub-national, national, regional, international). Co-operation includes public-private partnerships used, for example, to develop detailed regulation and to foster information sharing.

That co-operation emerged as a unifying theme reflects its unavoidable nature in the context of effective CIIP. The multiplicity of dimensions (e.g. economic, social, national security, technical, legal, etc.) and dependencies (e.g. digital dependencies, dependencies across actors, sectors and borders) mean that no single stakeholder can address the challenges associated with CIIP alone. Given that all stakeholders have limited responsibilities and capacities, dependencies translate into a complex web of relationships where each actor may be reliant on and responsible to each other for decision-making and action. Moreover, in many cases, the authority and the capacity to act in terms of resources and expertise vary across all actors. In a given situation, one actor may have responsibility but limited capacity whereas another may have greater capacity but less responsibility. As a result, co-operation emerges as fundamental to any solution. The updated Recommendation could articulate a strong high-level policy message around the theme of co-operation.

3.3. Only a whole-of-government approach can balance all interests at stake and ensure strategic vision

With such a multiplicity of dimensions, dependencies and co-operation arrangements, governments may face difficulties in maintaining an overarching strategic understanding of the situation and in ensuring that the competing interests at stake are appropriately balanced. The analysis of responses shows that governments address this challenge by integrating policies to protect essential services against digital security risk within their broader whole-of-government national risk management frameworks. The updated Recommendation should promote a whole-of-government approach in setting policies for the protection of essential services against digital security risk.

3.4. Different cultures and styles of government call for flexibility in policy implementation

Respondents provided a large amount of detailed information. An analysis of this information reveals commonalities with respect to the high-level objectives and content of policies as well as significant differences regarding the details of how policies are implemented at the domestic level. These differences are often the result of varied cultures and styles across governments such as degrees of governance centralisation and decentralisation as well as regulatory intensity (i.e. from mandatory to voluntary measures). An updated Recommendation would need to acknowledge the differences and build upon the commonalities.

4. Other suggestions for the updated Recommendation

The analysis of responses provided a large number of detailed suggestions for an updated Recommendation. On the basis of the analysis of these suggestions, the Recommendation should:

- Exclude national defence from its scope.
- Mention privacy protection.
- Go beyond just availability by explicitly mentioning integrity and confidentiality as well.
- Focus on what governments should do while recognising the national particularities related to how to do it (i.e. different cultures and styles of government). An example might be to avoid promoting a voluntary or mandatory approach, or promoting a centralised or decentralised model of governance.
- Distinguish services that are essential to the functioning of the economy and society from those that are essential to its prosperity.
- Address multi-dimensional interdependencies. For example:
  - recognise these interdependencies in the preamble
  - address intra-governmental co-ordination and co-operation across operators, sectors and borders
  - address cross-border aspects as they relate to cross-border dependencies.
- Consider human as well as technical aspects, such as personnel's knowledge and skills within operators and agencies with a mandate in this area.
- Include good practice with respect to public-private co-operation, such as incentives for participation in PPPs and the foundations of trust to foster PPPs.
- Reiterate and/or build on some of the main messages of the 2015 Security Risk Recommendation's regarding digital security risk management (e.g. promoting digital security risk management as a C-level responsibility).

The CIIP Recommendation contains good practice that continues to be valid and should be kept in the updated Recommendation. As additional guidance, the updated Recommendation could encourage governments to:

- Adopt a holistic approach where digital security risk management of essential services is part of national risk management.
- Build a framework step-by-step, progressively accumulating experience and expertise rather than trying to set up all the building blocks at once. Adopting a national digital security strategy and a national risk management framework prior to a detailed policy to protect essential services against digital security risk.
- Adopt a whole-of-government governance framework, including strong co-ordination mechanisms and clear allocation of responsibility, rather than promoting particular degrees of or modalities for centralisation/decentralisation.

- Adopt policies targeting operators that:
  - take into account their economic context
  - provide incentives for operators to better manage digital security risk and to integrate digital security risk management into their decision making related to the adoption of digital technologies (cf. 2015 Security Risk Recommendation)
  - encourage sharing of risk-related information
  - promote exercises and drills
  - consider prevention, response and resilience and address all-hazards rather than only intentional threats.
- Develop markets for digital security products and services e.g. through minimum standard requirements or PPPs to develop a trusted ecosystem of security services providers.
- Regularly review their policy framework on the basis of clear and transparent criteria.

Annex A. Summary and analysis of countries' responses

This Annex contains a summary and analysis of responses to a questionnaire sent to OECD member and non-member countries with regard to the proposed update to the CIIP Recommendation. It identifies suggestions that could feed into an updated Recommendation. Eighteen countries responded to the questionnaire representing a variety of regions, country cultures, sizes, and digital maturity: Belgium, Canada, Chile, Colombia, Czech Republic, Estonia, France, Germany, Japan, Korea, Norway, Poland, Russia, Spain, Sweden, Turkey, the United Kingdom and the United States. Input was also received from BIAC, CSISAC and ITAC at an early stage of the process (cf. Annex C).

The questionnaire included 27 open questions, most of which called for respondents to provide more detailed information. As a result, a vast amount of information was collected with varying levels of detail per question and per country. A general analysis showed that respondents' countries generally fall into one of three categories:

1) those with an "established" framework for critical information infrastructure protection (CIIP) that was adopted several years ago;
2) those with a recently adopted CIIP framework or are currently developing their first;
3) those planning to develop their framework.

These differences explain, to a large extent, the variations in the levels of detail provided by each country in their response for each question.

This Annex is structured around two sections. The first section examines responses related to the continued relevance of the CIIP Recommendation. To keep the analysis manageable, it was decided to focus on the identification of high-level trends in domestic CIIP policies. The second section examines the foundations for CIIP and policy frameworks in respondents' countries using a series of subsections. Each subsection ends with suggested changes for an updated CIIP Recommendation.

Continued relevance of the CIIP Recommendation

A majority of countries agree that the CIIP Recommendation should be updated to reflect the 2015 Security Risk Recommendation

Most countries agreed that the concept of CII, as defined in the 2008 CIIP Recommendation, is aligned with their understanding of CII and many of them used it to inform the development of their domestic policy. However, a majority of countries also agreed that the 2008 CIIP Recommendation should be updated to reflect the 2015 Security Risk Recommendation.

While supporting an update of the Recommendation, one country noted that the potential benefits from such a change are unclear. Most countries that do not support updating the Recommendation did not provide additional explanation to support their position. However, one noted that the CIIP Recommendation already implicitly focuses on economic and social prosperity and that the terminology differences are not important.

Evolutions in the policy landscape and in the environment are driving other suggested changes to the Recommendation. These include:

- Considering changes in the market structure of CI sectors resulting from deregulation. This includes the emergence of new operators, which may be smaller in size and not always sufficiently prepared for digital threats. It also includes more intense pressure on CI operators to reduce their operational costs including costs related to digital security measures.
- Providing a more holistic approach combining national risk management and CIIP.
- Further clarification of the meaning of "CIIP across borders" and "cross-border interdependencies".
- References to prevention, response and resilience.
- The importance of commitment to CIIP activities at enterprise management level (or C-level).
- The development of markets for digital security products and services through minimum standard requirements.
- The creation of a culture of trust among stakeholders, including for the exchange of sensitive information.
- Addressing the integration of Internet of Things (IoT) devices into the CI, and, more generally, the convergence or fusion of Information Technology (IT) and Operational Technology (OT), recognising that the OT and IT cultures and experts are different. In addition, references were made to industrial control systems (ICS).
- Continuous training of personnel in critical infrastructures as well as in government agencies with a responsibility in this area.
- Shared standards for a common understanding on impacts of digital security incidents.

Suggestions for the updated Recommendation

These elements confirm the widespread view that the CIIP Recommendation needs to be updated. They provide a series of suggested changes that should be taken into consideration when updating the Recommendation.

CIIP Foundations

A series of trends, challenges and issues create impetus for an update

Box A A.1. reports examples of respondents' perceptions of the most significant changes since 2008 in terms of the trends, drivers and challenges related to CIIP. The most cited trends and challenges were fast digital transformation and increased digital reliance of businesses and governments; increased frequency and severity of attacks on CII; the rise of state-sponsored attacks including digital sabotage and espionage; and the increased capacity of attackers.

Many countries underlined intentional threats but some also stressed unintentional incidents such as human errors resulting from the growing complexity of systems and lack of digital literacy of end users. Interestingly, only one respondent mentioned natural disasters among the most significant trends but other countries mentioned natural disasters in their responses to other questions and stressed that they follow an all-hazards approach.

Multi-dimensional interdependencies (i.e. across sectors, borders, government/business, civilian/military, etc.) were highlighted as challenges, perhaps resulting from the digital transformation of the economy and society given that it cuts across all economic sectors and areas of society.

Analysis

Multi-dimensional interdependencies are a key aspect of national risk management and have particular relevance to digital security. The presence of dependencies points to responsibilities also being interdependent (i.e. every stakeholder depends upon other stakeholders fulfilling their responsibilities). Co-operation is therefore necessary among interdependent stakeholders and appeared as an important cross-cutting theme in all responses. Dependencies are further discussed in Annex B.

References to sabotage and espionage suggest that while availability remains the main focus, integrity and confidentiality are becoming increasingly important. This may be driven by challenges related to the fast digital transformation of public and private sectors as well as enhanced risk from new technologies. This suggests a need for digital security risk management to be integrated into business decision making with a view to continuously and systematically assessing the pros and cons of adopting a new technology for economic and social activities.

The perceived importance of digital literacy and role of human error point to the human dimension, which relates to knowledge and skill acquisition.

Suggestions for the updated Recommendation

The updated Recommendation could address multi-dimensional interdependencies explicitly. For example, it could recognise these interdependencies in the preamble and address intra-governmental co-ordination and co-operation across operators, sectors and borders.

In addition, the updated Recommendation could:

- reiterate and/or build on some of the main messages of the 2015 Security Risk Recommendation's regarding digital security risk management
- explicitly mention availability, integrity and confidentiality
- promote an all-hazards approach rather than focus only on intentional threats
- consider human aspects, in addition to technical aspects, such the knowledge and skills of operators and agencies with a mandate in this area.

Box A A.1. Most significant trends, drivers and challenges related to CIIP (not by order of importance)

General context:

- limited understanding of digital security risk management despite threat increase and diversification; shortage of digital security experts; importance of enterprise management level (or C-level) commitment to digital security
- absence of a single regulatory and supervisory institution that addresses all critical infrastructures as well as slow pace of policy/legislative development
- convergence of digital and physical becoming a threat to national security; convergence of operational technologies (OT) with information technologies (IT)
- interdependencies across sectors, borders, public and private actors as well as military and civilian actors
- low digital literacy of end users and lack of public trust in the State.

Threat-related aspects:

- multiplicity of threat sources including criminals, States, hacktivists, and terrorists; development of organised crime online
- increased capacity of attackers due to the proliferation of sophisticated attack tools and services including via the underground market; development of digital weapons designed to target CIIs through state-sponsored attacks
- increasing likelihood of human management and operational error resulting in-part from growing ICT systems' complexity.

Aspects related to vulnerability and digital reliance:

- fast digital transformation of public and private sectors
- technology trends such as new storage environments; high adoption of smartphones; increased use of big data, artificial intelligence and augmented/virtual reality; rise of the IoT and SCADA/industrial control systems including for smart grids
- possible data exfiltration through a hardware backdoors
- insufficient security of SMEs.

Incident related aspects:

- increased frequency and severity of attacks on CII
- rise of sabotage targeting critical infrastructures
- destabilisation through actions of a digital nature
- digital espionage, targeting governments and intellectual property of national economic actors as well as mapping of critical infrastructures.

All respondents underline the strong relationship between CIIP and economic and social development

Summary of responses

All respondents agreed that CIIP is vital to economic and social development and the well-being of citizens although they express it in different terms. They recognise that CIIs support infrastructures are essential for basic social and economic functions and to "keep the country running". As noted by one respondent, "we now rely on critical information infrastructures for everything in our society. CIIP is not an end in itself, but rather facilitates economic and social development". Economic and social development depends on the information infrastructures that support essential services.

Respondents make the following additional observations[8]:

- Failure or deterioration of CIIs would have considerable detrimental impact on people's economic activities and living conditions. It could affect prerequisites for economic prosperity including: economic and social stability and confidence, the strength of the national economy as well as the country's international standing and reputation.
- The consequences of CII failure on public welfare at all levels (including the economy, government and society) always have to be taken into account in CIIP policymaking. A simple economic cost-benefit analysis from the perspective of an operator of CI/CII does not provide an appropriate approach for protection for the economy and society as a whole.
- The relationship between CIIP and economic and social development requires appropriate coordination and co-operation across public administrations, the private sector and citizens. Furthermore, public-private co-operation is crucial for CIIP as most operators of critical infrastructures are owned and operated by private companies.
- Economic development hinges on interdependent and interconnected information systems across critical infrastructures. However, some critical infrastructures (e.g. finance, energy, transports, telecommunications) are more tangibly related to economic and social development than others.
- Information systems supporting CIs are sometimes managed by foreign corporations.

Analysis

The responses confirmed the importance of co-operation and co-ordination across all categories of actors. They also showed that CIIP should be approached from a broad and holistic perspective rather than that of a single operator, sector, or angle (e.g. national security). This suggests that a whole-of-government approach would be most appropriate as it ensures that all the interests are taken into account, appropriated balanced and addressed. It also facilitates effective co-ordination and co-operation between stakeholders.

The fact that some critical infrastructures are more directly related to economic and social development than others suggests that some infrastructures have more direct "national security" than "economic and social" importance (e.g. defence infrastructure). A major evolution since 2008 is the increasing importance of national security as one of the dimensions of digital security policy making (OECD, 2012[6]), (OECD, 2015a[7]). Within

digital security policy making, CIIP is often characterised by an overlap between socio-economic and national security dimensions. This suggests that a good governance framework should aim to ensure that both aspects reinforce rather than undermine each other.

The current definition of CII in the 2008 Recommendation includes, "systems and networks, the destruction of which would have a serious impact on the safety, security, of citizens". This could be understood as including systems supporting, for example, national defence, which is beyond OECD's mandate.

Suggestions for the updated Recommendation

Co-operation and co-ordination as well as the need for a holistic and whole-of-government approach could form the cornerstone of the updated Recommendation. The updated Recommendation should exclude national defence from its scope.

The national digital security strategy and national risk management frameworks form a basis for policy frameworks, including the definition of 'criticality'

Summary of responses

Descriptions of countries' policy frameworks show that CIIP policy is generally developed after the adoption and on the basis of both a national risk management policy framework (i.e. framework to protect essential services / critical infrastructures) and a national digital security strategy.

Respondents' definition and understanding of CI and CII are all based on the severity of the consequences of disruption on an essential/critical part of the national economy or society, including loss of life. There is however a broad range of criteria to define the severity of consequences with some countries being more specific than others (e.g. with figures such as casualties above a certain threshold, economic loss higher than a given percentage of GDP, disruption of essential services affecting more than a number of people, etc.). Specific cross-sectoral criteria sometimes take into account interdependencies across infrastructures. Although it is not explicitly stated in the responses, the criteria used to define criticality are likely to correspond to those of more general national risk management.

Some countries also consider "operators of vital importance" in addition to organisations that are essential for the functioning of the economy. These organisations are considered to be essential to the economic potential of the country in light of their contribution to the economy. One country noted that further implementation of the NIS Directive may increase this trend as EU members will have to identify operators that are essential to the functioning of the economy and the EU single market.

Analysis

Responses consistently reflected the history of the CIIP concept, which was developed in the mid-2000s as an extension to the concept of Critical Infrastructure Protection (CIP), and now often also called national risk management. However, the fact that criteria for defining criticality are the same for national risk management and CIIP suggests that CIIP and national risk management policy are tied-up at the policy and operational levels with CIIP forming the digital tier within the national risk management framework.

CIIP policy should not be understood as an isolated area but rather it should be developed on the basis of and integrated with:

1) a broader framework to protect essential services or critical infrastructure;
2) a national digital security strategy.

The national digital security strategy should consistently elevate the importance of digital security within the broader policy landscape rather than create a new policy silo. Countries should first develop their national risk management framework and national digital security strategy prior to their CIIP framework (cf. page 26 below regarding the need for a step-by-step approach).

The efficient integration and co-ordination of these policy building blocks is likely to depend on how policies are developed and implemented. Here again, a holistic whole-of-government governance framework supporting effective co-operation and coordination seems particularly relevant.

A distinction should be made between services that are considered as essential for the *functioning* of the economy and society and those that are essential for the *prosperity* of the country without being necessarily essential for its functioning. Operators of the latter services could include, for example, some key organisations in sectors which contribute significantly to the GDP without being critical infrastructures (e.g. a car manufacturer, a large mining company, an entertainment group, a multinational in cosmetics, etc.). This echoes the distinction already made in the CIIP Recommendation between information components supporting *critical* infrastructures and information infrastructures *essential* to the national economy (cf. Box A A.2). Policy measures addressing services essential for a country's prosperity could be based on the same general high-level framework but adjusted according to their lower level of criticality.

Suggestions for the updated Recommendation

The updated Recommendation could emphasise the need for an integrated approach whereby CIIP is a component of national risk management, and for a holistic and whole-of-government governance approach to CIIP. Among essential services, the updated Recommendation could distinguish between those that are essential to the functioning of the economy and society and those that are essential to its prosperity.

Box A A.2. Identification of CII according to the 2008 CIIP Recommendation

Critical information infrastructures, hereinafter "CII", should be understood as referring to those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy.

National CII are identified through a risk assessment process and typically include one or more of the following:

- information components supporting critical infrastructures; and/or
- information infrastructures supporting essential components of government business; and/or
- information infrastructures essential to the national economy.

Source: OECD, 2008

Respondents follow an "information infrastructure approach", a new trend called a "service approach", or a mix of both

Summary of responses

Three groups of countries can be distinguished. Countries with:

- a focus on the protection of critical information infrastructure ("information infrastructure approach")
- a focus on the protection of essential services, functions or activities against digital security risk ("service approach")
- a mix of both (hybrid approach).

The terms "essential" and "critical" are often used interchangeably. However, "essential" seems to be more associated with services while "critical" seems to be more associated "infrastructure".

Countries that developed a policy framework a decade ago generally follow the information infrastructure approach, which is in line with the 2008 CIIP Recommendation. According to this approach, the concept of critical information infrastructure extends the pre-existing concept of stove-piped critical infrastructures such as energy, finance, health, etc. to the, "information systems and networks the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy".

Countries with a more recent framework generally follow a "service approach". They focus on services, functions or activities that are critical to the economy and society rather than on the information infrastructure assets that support these services. The notion of infrastructure sometimes appears in the description of their framework but it is less prominent than that of function or service. These countries do not necessarily use the "CII" concept in their framework. Rather, they understand it as one particular risk that must be taken into account within the broader assessment of risks to essential services.

Many European countries' responses focussed on "essential or vital services/activities", often making an explicit reference in their responses to the EU Directive 2016/1148 on security of network and information systems ("NIS Directive"). The NIS Directive defines operators of essential services as entities, "providing a service which is essential for the maintenance of critical societal and/or economic activities"[9]. In the NIS Directive, the terms "services" and "essential" appear 158 and 109 times respectively, while "critical" and "infrastructure" only appear 7 and 11 times respectively. The term "critical information infrastructure" does not appear.

Nevertheless, the focus on essential services is not limited to European countries. For example, one non-European country stressed that it is performing a strategic policy shift from securing the critical information infrastructure to assuring continuous critical service provision.

Some countries follow a "hybrid approach" which borrows from both the “critical information infrastructure approach” and from the “service approach”. Some of them, particularly European countries, indicate that they are transitioning from critical infrastructure to critical or essential service protection.

Analysis

The emergence of a "service approach" is the most fundamental change since 2008 that was identified in the responses. It echoes the transition from the 2002 Security Guidelines to the 2015 Security Risk Recommendation where the focus of digital security shifted from information systems and networks (i.e. the infrastructures or assets) to the economic and social activities (i.e. the services or functions) that rely on them.

European countries that follow a hybrid approach might be transitioning from the older information infrastructure approach to the more recent service approach in order to implement the NIS Directive. This might also suggest that their overarching national risk management framework, based on the infrastructure approach, is not aligned with the more recent and service-based NIS Directive.

Overall, the distribution of countries across information infrastructure, service and hybrid approaches points to the service approach being a recent trend and that some countries are progressively converging towards it.

There seems to be a misalignment between the CIIP term and concept and the CIIP policy frameworks that countries actually have in place. The CII and CIIP terms and concepts do not seem to be used by a majority of countries in the development of their domestic policy framework.

Suggestions for the updated Recommendation

This analysis suggests that the updated Recommendation could focus on the protection of critical components of essential services rather than CII at a higher level. This would create greater alignment with the 2015 Security Risk Recommendation.

A discussion on terminology would be needed to distinguish between critical, essential and vital as well as services, functions and activities. These terms may carry different meanings in different countries.

The Recommendation should aim to help policymakers develop an effective policy framework tailored to their culture and style of government rather than prescribe or advocate the use of specific terms when several are relatively equivalent. A separate explanatory note could clarify these aspects.

Use of the concept of CII does not seem to be widespread in policy making

Summary of responses

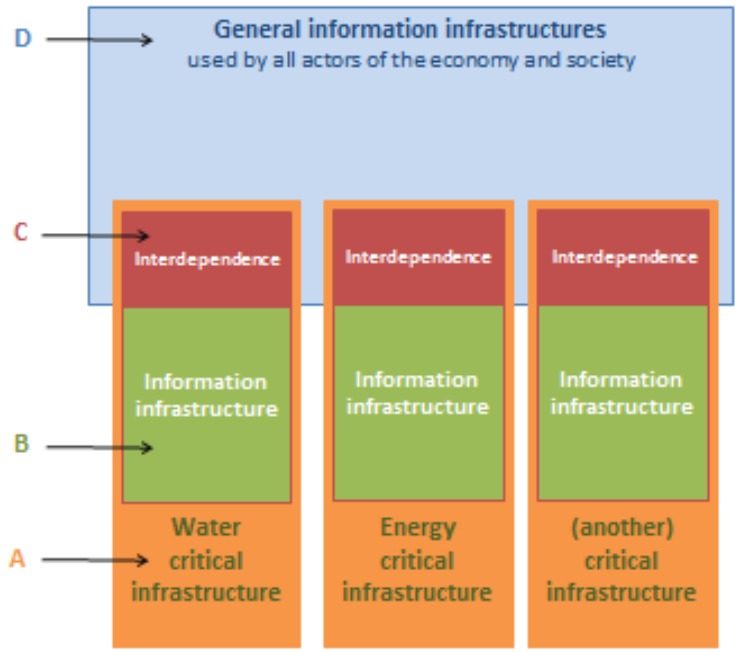
The questionnaire included three questions aimed at understanding the scope of CIIP frameworks and the extent to which frameworks address digital security risks:

- to information infrastructures that are specific to the operation of critical infrastructures (Cf. Figure A A.1, B, area in green); or
- that arise from the use of the general information infrastructures (such as the Internet, public communication networks, etc. (Figure A A.1, C, red boxes); and
- to the general information infrastructures used by all actors of the economy and society (e.g. the Internet, parts of it, particular Internet services, etc., cf. Figure A A.1, D, blue box).

Almost all countries replied “Yes” to these questions. From the details provided in the responses, it does not seem that the distinction between C and D is driving specific policy

measures. Policy frameworks generally address the information infrastructure within or supporting critical infrastructures (B) by adopting sector-specific measures.

Figure A A.1. Interdependencies



Note: This figure illustrated questions Q2.7-Q.2.9. The orange boxes A represent critical infrastructures, taking the water and energy sectors as examples. The green boxes B represent information infrastructures that are specific to the operation of each critical infrastructure. The red boxes C represent interdependencies, i.e. the part of the general information infrastructures (such as the Internet, public communications networks, etc.) on which critical infrastructures rely. The blue box D represents the general information infrastructures used by all actors of the economy and society

Analysis

Responses to these questions suggested that Figure A A.1 was not well understood by most respondents, perhaps because it was too complex or did not appropriately reflect the concepts used by CIIP policy makers. However, Figure A A.1 flows logically from the concept of CII, which supposes that critical information infrastructure is composed of the critical elements found in B, C and D. According to this logic, C represents the dependency of critical infrastructures such as energy, finance, etc. on general information infrastructures such as the Internet.

The fact that these distinctions did not seem to really make a difference in respondents' policy frameworks suggests that the concept of CII is not systematically used to develop policy in this area. Indeed, some responses suggested that the subtleties of the CII concept are not always understood.

Suggestions for the updated Recommendation

It appears that policymakers' understanding and application of the concept of CII is limited. This might suggest the need to evolve towards a simple notion, such as the protection of essential services against digital security risk.

Policy frameworks

New CIIP policy frameworks tend to be adopted step-by-step and existing ones evolve in response to a changing environment

Summary of responses

Many countries with a CIIP framework that was initially designed several years ago are updating it to adjust it to their national digital security strategy, which has also generally evolved over time. In the European Union, the NIS Directive is driving some EU members to adopt a new or update their existing framework.

Countries' responses about their priorities and goals for the future vary according to the maturity of their framework. Many European countries mention the implementation of the NIS directive as a key objective. Countries without an existing framework plan to start with the adoption of a basic CIIP framework comprising the identification of CII and responsible organisations, the establishment of a new CERT/CSIRT, vulnerability testing of government systems, awareness raising at executive level, identification of interdependencies, etc. Countries with more developed experience of CIIP and more mature digital security policy underline other aspects such as: stepping up PPPs, providing technical support to operators or auditing their risk management.

Analysis

Overall, responses showed that governments are taking a step-by-step approach to the development of their CIIP framework. They first adopt a digital security strategy and a national risk management framework. They then adopt the fundamental elements of a CIIP framework such as governance and co-ordination mechanisms. The most mature improve and update their framework by adding new building blocks through an iterative cycle of improvement.

Suggestions for the updated Recommendation

The Recommendation or its explanatory document could suggest a sequential process for building a CIIP framework. This would emphasise the need to change or extend the framework based on the progressive accumulation of experience and expertise rather than attempting to set-up all the building blocks at once.

While the scope and scale of the CIIP policies are relatively similar, frameworks vary according to factors such as culture and style of government

Summary of responses

The comparison of CIIP frameworks reveals many differences across countries, resulting from the national context. This can include the structure, culture, style of government, legal system, as well as factors such as co-operation in a regional framework (e.g. European Union), the socio-economic background and history/stage of policy development in this area. It is possible that other factors also play a role such as the country's size, level of digital maturity and dependency as well as maturity of policy for the protection of critical infrastructure.

Despite these differences and taking into account the fact that some countries started earlier than others, the scope and scale of the CIIP policies are relatively similar. A few responses, however, focused primarily on the telecommunications sector, which suggests that they follow a different, infrastructure-focused approach.

Analysis

There is no one-size-fits-all policy framework that would adequately satisfy the needs of all countries. High-level recommendations should therefore take the form of flexible principles that countries can translate into appropriate policy frameworks according to their own culture and style of government.

Suggestions for the updated Recommendation

An updated Recommendation should provide high-level guidance as to what governments should do to protect CII while leaving scope for countries to develop and implement their CIIP policies in line with their national particularities.

A whole-of-government approach was widespread though degrees of centralisation and decentralisation varied

Summary of responses

Countries demonstrate leadership and commitment by assigning CIIP policy responsibilities to lead organisations through legislation or a combination of a national risk management policy framework and a national digital security strategy. Legislation is frequently seen in countries with a CIIP governance framework that was adopted less than 5 years ago and is often planned by countries that are currently developing or revising their framework.

Government agencies' CIIP policy responsibility generally includes cross-sector, high-level policy development and co-ordination; sector-specific policy development; development and/or adoption of standards; a national CERT function; and supervision of operators.

All respondents adopted a whole-of-government approach with strong co-ordination mechanisms. However, the degree of centralisation/decentralisation varied across countries. In some countries, a single lead organisation is responsible for addressing all sectors and supervising operators, in co-ordination with relevant sector-specific ministries and agencies. In other countries, sector-specific ministries and agencies are responsible for addressing CII in their sector with the support of a lead organisation that develops the overarching strategy and fostering cross-sector co-ordination. In some cases, the lead organisation also provides technical assistance to operators and/or agencies.

Analysis

The responses suggested the widespread acceptance of a whole-of-government framework that establishes effective co-ordination between stakeholders. This provides the government with a means to include digital security risk in its overall national risk assessment. Such a framework is also essential for the elevation of the level of digital security across sectors if it takes into account dependencies and interdependencies. It provides a means to balance and reconcile potentially competing policies and objectives such as economic and social prosperity and national security, digital security and innovation, etc. Lastly, it facilitates the efficient use of scarce resources across sectors such as digital security expertise.

Nevertheless, responses also showed that there is no one-size-fits-all approach to a whole-of-government framework. In particular, countries' style of government, culture and history appear to play a key role in determining the most appropriate degree of centralisation/decentralisation given the specific context.

Suggestions for the updated Recommendation

The Recommendation could focus on the need for a whole-of-government governance framework, including strong co-ordination mechanisms and clear allocation of responsibility, rather than promoting particular degrees of or modalities for centralisation/decentralisation.

Incentivising operators to enhance digital security risk management and foster information sharing can be achieved in a variety of ways

Summary of responses

In general, respondents recognised that operators of CIIs are responsible for the security of their information infrastructures. However, policy frameworks are not limited to expressing, clarifying or strengthening this responsibility. Governments' intervention in this area is justified on the grounds that governments have some responsibility to ensure the continuity of essential services that depend upon CII. Nevertheless, the nature of their intervention takes many forms and uses many tools including: standards, legal obligations, regulation, co-regulation, encouragement of self-regulation, crisis management assistance and technical support, etc.

All countries are creating conditions for CII operators to foster the: *i)* adoption of enhanced digital security risk management; and *ii)* sharing of risk-related and/or best practice information and/or reporting of incidents.

Some respondents favour a *mandatory* approach to foster strengthened digital security risk management by operators. Obligations vary from flexible and principle-based to more prescriptive requirements, such as the submission by operators of their digital security risk management plans. Mandatory requirements are often combined with supervision through inspection or audit. Other respondents favour a *voluntary* approach for strengthening the adoption of good practice. Measures include: the development and promotion of standards, establishment of certification schemes, organisation of digital security exercises, etc. One country tasked its national standards body to work with private sector to collaboratively develop a standard and best digital security risk management practice, which operators are encouraged to voluntarily adopt.

Many countries encourage voluntary information sharing between the public and private sector, and within the private sector, for example through PPPs (see below) and funding for information sharing and analysis organisations. EU respondents are adopting new regulation to implement article 14 of the NIS Directive according to which operators of essential services will have to notify significant incidents to the relevant national authority (cf. Box A A.3). Two countries had enacted legislation to that effect prior to the final formal adoption of the Directive.

Box A A.3. EU NIS Directive, Article 14 "Security requirements and incident notification"

1) Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed;
2) Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services;
3) Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability. […]

Source: EU NIS Directive

Respondents also supported the organisation of exercises to improve digital security risk management across the broader spectrum of crisis management. Some countries mention cross-border exercises. Exercises tend to be mentioned in national digital security strategies, legislation, action plans or other policy documents. Their goals include improving risk assessment; facilitating swift response to incidents and identifying flaws in incident response procedures; fostering identification of points of contacts; enhancing cross-sector and public-private co-operation; and training of strategic decision makers.

Analysis

The choice of approaches used to encourage operators to manage digital security risk is likely to depend on the country's style of government, culture and history. Other factors might include: the extent to which a given sector is already regulated, the number, size and geographical distribution of operators to be overseen, the resources available to the lead organisation, consistency with the broader policy framework to manage other risks, etc.

The CIIP Recommendation mentions the need for governments to promote good security practice at the national level, to encourage information sharing, and to use exercises as part of "a system of measurement to evaluate and appraise measures in place".

Suggestions for the updated Recommendation

The Recommendation could focus on the need to encourage better digital security risk management practice across stakeholders. Building on the 2015 Security Risk Recommendation, it could focus on incentives for operators to strengthen their digital security risk management and to integrate digital security risk management into their decision making related to the adoption of digital technologies. The Recommendation could encourage information sharing and promote exercises. However, it should not promote a voluntary or mandatory approach.

Public-private co-operation plays an essential role in CIIP frameworks

Summary of responses

Throughout the responses, public-private co-operation appears as an essential component of CIIP frameworks. Trust is often mentioned as essential for effective PPPs. Public-private partnerships (PPPs) are used at both the policy making and operational levels.

At the policy making level, PPPs facilitate the establishment of trust between the government and private sector. They support the development of the policy framework including identification of good practice that operators should follow. In some countries, they help align efforts of private operators, state and local (i.e. sub-national) governments. Some respondents that have adopted or plan to adopt legislation targeting operators of critical information infrastructures follow a co-regulation model with voluntary PPPs to define the details of the regulation or specific requirements with the private sector. Such PPPs aim to take into account operators' expectations and constraints to avoid creating unnecessary burdensome requirements. They also aim to build trust among participants by establishing reciprocal benefits whereby the government gains a better understanding of the field and improved relationships with operators and operators benefit from a more realistic regulation that better fits their needs. Furthermore, in some cases, the PPP includes government actors such as sectoral regulators and also provides a venue for discussions among operators without government representatives. One respondent underlined the possibility of the digital security agency providing direct assistance to operators in case of crisis being a key incentive for operators to build a trust relationship with this agency and participate in the PPP.

At the operational level, PPPs help achieve various objectives including mapping out the essential digital assets, developing response plans for exercises, sharing best practice and sector-specific good practice, training, identifying dependencies, and sharing risk-related information. One country mentioned the establishment of a PPP to develop an ecosystem of trusted commercial digital security services.

PPPs are clearly important in most responses but apparently not always translated into concrete initiatives. Variations across countries range from very broad PPP frameworks that sometimes cover both national risk management and CIIP, addressing all critical sectors and many aspects of CIIP including governance structures, sub-groups, regional activities, etc.; to the simple organisation of conferences where private sector input is collected. As in many other aspects of CIIP, the extent of public-private co-operation seems to vary according to the maturity of the country's CIIP approach.

Analysis

The strong support for PPPs is consistent with the CIIP Recommendation and with the recognition that CIIP is a complex and dynamic area that requires policy agility and approaches that need to be tested over time. A government-centric and rigid approach is unlikely to address CIIP in a manner that manages the risk without hindering digital transformation in essential sectors.

Further exploration of the conditions that lead to greater trust in public-private co-operation would be beneficial. It could seek to understand the various approaches across OECD countries by identifying good practice, including in the creation of trusted relationships across partners, and identifying the modes of national governance that facilitate or hinder public-private relationships.

Suggestions for the updated Recommendation

These findings suggest that the updated Recommendation could:

- encourage PPPs for a variety of purposes
- include good practice with respect to public-private co-operation such as incentives for participation in PPPs and foundations for trust to foster PPP
- address PPPs in the development of a trusted ecosystem of security services providers

Further work would be useful to identify good practice related to PPPs.

All but three countries agree that a domestic market has emerged to address the demand for products and services for CIIP

Summary of responses

Several countries underlined the importance of public policy to stimulate the market for digital security products and services. For example, some indicated that the requirement in the EU NIS Directive for operators to adopt "state of the art" technical and organisational digital security risk management measures (cf. Box A A.3) is expected to have a positive effect on the market. According to one country, digital security is similar to most security-related areas such as health, fire and road safety: a balanced regulation of digital security should stimulate the demand side. One country also underlined that the co-drafting of regulation can play a key role to stimulate demand. However, regulation is not the only way to stimulate the market. One country noted that public policy strives to support continued research and innovation on products and services that help protect CII.

Detection, response and certification products and services were among the most frequently mentioned topics in the responses. Some countries place emphasis on products, others on services (incl. training, certification services, etc.) and some on both. One (large) country mentioned the rise of domestic security products and services exports, while another (smaller) country highlighted that the market is international. One country noted that government products and services certification schemes can be both neutral and effective. Public procurement strategies were pointed out as a possible lever for the development of the market while ensuring that the government leads by example. One country underlined that the government can play a key role in aligning higher-education curricula with the skills required as a consequence of CIIP policies.

Suggestions for the updated Recommendation

These findings suggest that the Recommendation could call for CIIP policy to encourage the development of a vibrant market for digital security products and services and indicate good practice in this area. This could include: the need for an open market, the role of public sector demand and private sector access to certain risk-related data and information currently in the hands of the government.

Half of respondents agree that privacy protection needs to be addressed in CIIP policy frameworks in the future.

Summary of responses

Half (nine) countries answered that privacy protection needs to be addressed in CIIP policy framework in the future. These respondents underlined the importance of privacy protection in relation to digital security policy in general and with respect to the protection

of CII in particular. One respondent indicated that privacy protection can be an obstacle to informing owners of known infected systems. Another stressed that sensitive data should be anonymised. One country underlined the need for transparency regarding how privacy is protected as CIIP frameworks are implemented. Two respondents underlined the importance of privacy but understood it as synonymous with confidentiality of information in general rather than as the protection of information related to individuals (personal data).

Six countries responded that privacy protection does not need to be addressed in CIIP policy frameworks in the future. Although they did not provide explanations the fact that five of them are members of the European Union suggests that they consider the existing privacy regulation is sufficient and thus they do not see a need for privacy to be specifically integrated into CIIP-related frameworks.

Analysis

The 2008 CIIP Recommendation does not mention privacy nor does it include a reference to the OECD Privacy Guidelines. The increased perception of the importance of privacy protection in this area is therefore a new development since 2008. Trends such as the increasingly important role of personal data for the management of essential services, technologies such as big data analytics and artificial intelligence, and the general data-driven digital transformation of the economy and society are likely to lead to increasing numbers of privacy issues in the context of CIIP in the future.

Suggestions for the updated Recommendation

The updated Recommendation could mention privacy protection and refer to the OECD Privacy Guidelines.

Most countries refer to the importance of various forms of bilateral and multilateral international co-operation

Summary of responses

Most countries mention bilateral, regional and international co-operation. Activities vary from operational co-operation such as joint risk assessment related to shared critical infrastructure, capacity building, best practices sharing, CERT/CSIRT co-operation**,** joint threat information exchanges, organisation and participation in regional and international exercises, participation in international and regional networks for monitoring, warning and incident response, and training. Co-operation may take place through CII-specific arrangements; through broader arrangements addressing critical infrastructure protection; or through digital security co-operation. Many countries share information publicly about their national agencies involved in CIIP and have identified a national point of contact.

Within the EU, most co-operation activities are expected to take place through the Co-operation Group and network of national CSIRTs established by the NIS Directive (cf. Box A A.4. Some EU members also mention the European Programme for Critical Infrastructure Protection (European Commission,(n.d.)[8]) as well as the Technical Assistance and Information Exchange instrument of the European Commission (TAIEX) (European Commission,(n.d.)[9]).

Many responses from non-EU members mention other international fora including APEC, ASEAN (ASEAN, 2015[10]), Meridian Process, NATO, NorCert (Northern European countries) and OSCE. One country also mentioned the BRICS (BRICS, 2015[11]), (BRICS, 2016[12]) and the Shanghai Cooperation Organisation. In general, these responses do not

always clearly distinguish general co-operation on digital security from specific co-operation focusing on CIIP.

In a response to another question related to the Recommendation, one country pointed at the lack of clarity of the expression "CIIP across borders" and questioned the need for special international co-operation mechanisms or activities related to CIIP that would promote specific CIIP activities that are not already covered by more general, existing international co-operation initiatives.

Analysis

Responses show that countries address many aspects covered by the second part of the Recommendation, which focuses on the protection of CII across borders. However, the content of responses as well as criticisms regarding the lack of clarity of that part of the CIIP Recommendation suggest that the updated Recommendation could address cross-border aspects in a different manner and perhaps with more precision.

Suggestions for the updated Recommendation

The updated Recommendation could address cross-border aspects in relation to cross-border dependencies.

Box A A.4. NIS Directive Co-operation Group and CSIRT Network

The Cooperation Group will be composed of representatives of Member States, the Commission and the European Union Agency for Network and Information Security (ENISA) with the European Commission acting as secretariat. It will provide guidance for CSIRTs Network; Assist Member States in capacity building; Support Member States in the identification of operators of essential services; Discuss incident notification practices; Discuss standards; Engage with relevant EU institutions and bodies; Evaluate national strategies and CSIRTs (on voluntary basis); and Facilitate information and best practices sharing on risks, incidents, awareness-raising, training, and R&D.

The CSIRTs Network will be composed of representatives of the Member States' CSIRTs and CERT–EU (the Computer Emergency Response Team for the EU institutions, agencies and bodies). The Commission will participate in the CSIRTs network as an observer. ENISA will provide the secretariat and actively support the cooperation among the CSIRTs.

The CSIRTs Network will exchange information on CSIRTs services, operations and cooperation capabilities; exchange and discuss information related to incidents (on request and voluntary); identify a coordinated response to an incident (on request and voluntary); support cross-border incident handling (voluntary); explore further forms of operational cooperation; inform the Cooperation Group of its activities and requesting guidance; discuss lessons learnt from exercises; discuss issues relating to an individual CSIRT (on request); and issue guidelines on operational cooperation.

Source: European Commission, 2016

Most respondents with a framework in place review it regularly though establishing clear metrics for assessing their effectiveness remains challenging

Summary of responses

One third of respondents regularly review their policy framework. When indicated, time intervals range from 1 to 5 years and are often aligned with reviews of digital security strategies or action plan, and/or plan for national risk management policy. Other respondents have recently developed or are developing their policy framework and therefore have not yet set the review process. Some countries refer to an irregular review process or answered that they have no review process.

To measure the effectiveness of the policy framework, some countries use quantitative indicators such as the number and severity of incidents, the number of instances of information sharing or the number of operators' staff participating in cross-sector exercises. Some countries also use semi-quantitative measures such as the results of operators' compliance audits. Some countries recognise the challenge of defining specific quantitative measurement and instead make a qualitative evaluation of their policy framework on the basis of exchanges with the relevant communities. For example, they seek to understand whether dependencies and interdependencies are known and capacity gaps have been identified.

Analysis

The regular review of an existing policy framework is considered good practice. However, some responses suggested that it can be challenging to develop and adopt objective criteria for the accurate assessment of CIIP policy frameworks.

Suggestions for the updated Recommendation

The updated Recommendation should call for a regular review of the policy framework on the basis of a clear and transparent criteria.

Annex B. Dependencies and interdependencies

Dependencies and interdependencies affect all components of risk (e.g. threat, vulnerability, consequences) as well as the resilience and performance of risk reduction measures. They have a multiplicative effect on risk and lead to a level of complexity that masks many systemic risks (Petit et al., 2015[13]). They are therefore essential to critical infrastructure protection and should be part of national risk assessment (OECD, 2014[14]).

A dependency is often defined as a unidirectional relationship between two assets where the operations of Asset A affect the operations of Asset B. An interdependency is a bidirectional relationship between two assets where the operations of Asset A affect the operations of Asset B, and the operations of Asset B then affect the operations of Asset A. (Rinaldi, Peerenboom and Kelly, 2001[15]); (Petit et al., 2015[13]); (Setola and Theocharidou, 2016[16]). Literature on the subject generally distinguishes different types and classes dependencies as well as various dimensions that can affect them such as the operating environment and the type of failure.

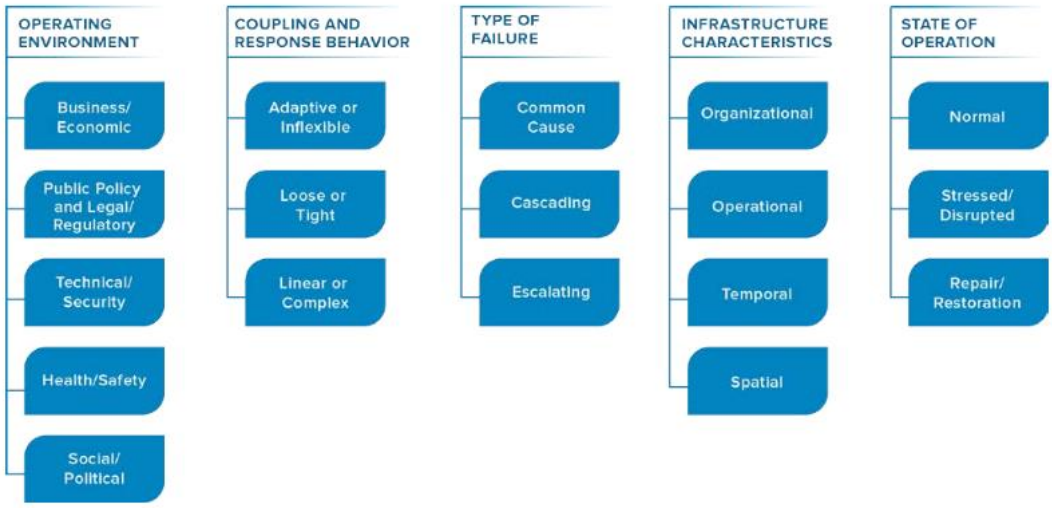
The interactions between critical infrastructure and its environment can be characterised into three categories:

- *Upstream dependencies*: The products or services provided to one infrastructure by another external infrastructure that are necessary to support its operations and functions.
- *Internal dependencies*: The interactions among internal operations, functions, and missions of the infrastructure. Internal dependencies are the internal links among the assets constituting a critical infrastructure (e.g., an electric generating plant that depends on cooling water from its own onsite water well).
- *Downstream dependencies*: The consequences to a critical infrastructure's consumers or recipients from the degradation of the resources provided by a critical infrastructure.

In addition, the connections among critical infrastructure assets are multidimensional, adding to their complexity. (Rinaldi, Peerenboom and Kelly, 2001[15]) propose the following five dimensions to characterise dependencies (and interdependencies) among critical infrastructure. They include, in particular, the *type of failures* affecting a dependency:

- *Common cause failure* – Simultaneous disruption of two or more infrastructure.
- *Cascading failure* – Disruption of one infrastructure subsequently causes a disruption in the second infrastructure. This type of failure is also called the domino effect.
- *Escalating failure* – Disruption of one infrastructure exacerbates an independent disruption of a second infrastructure. This type of failure is also called the snowball effect.

Figure A B.1. Five dimensions to characterise dependencies



Source: Based on Petit et al., 2015.

Two dimensions of "digital dependencies" could be reflected in the updated Recommendation because they underlie essential policy principles such as the need for co-operation and co-ordination and the integration to national risk management. The first builds on the type of failure. Three types of failures can be considered as characteristic of digital dependency and important for policy making:

- *Common cause failure*. A vulnerability affecting a digital component on which several or all essential services depend could be exploited and cause massive chaos and damages simultaneously across the economy. Such vulnerabilities could for example affect software, as in the Wannacry and NotPetya attacks; microprocessors or other hardware components, as illustrated by "Spectre" and "Meltdown"; or essential elements of the core Internet, such as the Domain Name System, Internet Exchange Points or Certificate Authorities. Although it did not affect critical infrastructures, the 2016 massive Denial of Service attack against the domain name provider Dyn took down access to numerous popular websites. Interestingly, vulnerabilities could affect digital assets operated by essential service providers (e.g. servers, data centres, SCADA systems, industrial IoT devices, etc.) as well as by end individuals, such as smartphones, autonomous vehicles or consumer IoT devices.
- *Digital propagation failure*. Another type of digital dependency is when a digital security threat to an operator of essential service successfully propagates to other operators, within the same and/or in different sectors, eventually causing damages to a large range of services, meeting the criteria of national criticality. A striking illustration of this possibility is the famous Stuxnet worm, discovered in 2010, which was initially designed to specifically target a nuclear enrichment facility in Iran and infected approximately 100 000 hosts in over 155 countries. Fortunately this occurred without incurring damages beyond its intended target.
- *Cascade failure* or digitally-caused non-digital cascade. A third type of dependency is when the disruption of the delivery of an essential service caused by a digital security incident cascades onto another essential service, subsequently causing a

disruption in its delivery. For example, a digital security incident could cause an electricity outage, which in turn would disrupt transport systems and hospitals in the outage's geographic area. This could cause disruptions of other essential services, etc. In this case, the digital security incident would act as the root cause of knock-on effects – propagating a disaster along a chain of interdependent essential services. However, the digital security incident itself would not directly affect the second-level services.

The second important dimension of dependencies results from the globally interconnected nature of digital technologies that creates dependencies across borders which may arise in combination with the above mentioned dependencies across services. The 2016 denial of service attack on Dyn demonstrated this kind of dependency as access to sites from Europe was affected by an incident taking place in the United States.

A national risk assessment that takes into account digital dependencies is likely to recognise that certain digital services can match the criteria of national criticality set in the broader national risk management framework. Historically (i.e. before the Internet), these would have been the "telecommunications operators". Today, they are likely to also include services such as top level domain name registries, Internet exchange points or some cloud services.

Annex C. Input from BIAC, CSISAC and ITAC

Input from BIAC, CSISAC and ITAC was received at an early stage of the review process. These elements, summarised below, suggest additional perspectives for the revision of the CIIP Recommendation:

With respect to the general context:

- The IoT, cloud and big data are major technical changes since 2008 (BIAC).
- Effective CIIP framework should consider risks of physical disruption, moral outrage and lose of trust derived from disruptions of critical infrastructures and services (CSISAC).
- CIIP has become a priority as a result of our societies' digital reliance. The disruption of CII could harm democratisation processes and trust in democratic countries, as well as efforts towards more social inclusion (CSISAC).
- CIIP should consider confidentiality and integrity in addition to availability (CSISAC).

With respect to the definition of CII:

- A clear definition of CII is an important first step in developing policy principles to foster its protection (ITAC).
- The definition of the CIIP Recommendation is still largely relevant and useful but would benefit from the addition of the concept of "provision of essential services" (ITAC).
- Best practices and/or some other guidance for identifying CII could be included in the Recommendation. For example, the OECD could establish a set of criteria for identifying CIIs that focuses on safeguarding essential services by protecting their associated information infrastructures. All stakeholders should understand the definition of CII, how to identify it in practice, and how best to take steps to protect it (ITAC).
- Overly broad and non-risk based definitions of CII that would subject commercial services to unnecessarily burdensome obligations and would inhibit innovative approaches to digital security should be avoided (BIAC).
- CIIP should consider the effects of CII disruption on all users, including vulnerable ones or in an irregular situation (CSISAC).

With respect to public-private co-operation:

- Public-private co-operation is essential for CIIP in part because of the rapid pace at which technologies and security threats are evolving (BIAC).
- Trusted relationships are essential for effective public-private co-operation. In particular, disclosures related to CIIP by organisations often contain sensitive or proprietary information requires enhanced guarantee of confidentiality and, more generally, digital security (BIAC).

- Liability and threat of legal repercussions are obstacles to national and international information sharing. Information sharing regimes should be voluntary and protect sensitive company information from being used for regulatory or other legal action (BIAC).
- Public-private research and development should be encouraged (BIAC).
- The Recommendation should emphasise the need for co-operation and collective responsibility among all stakeholders, not just the government and CII owners and operators. All stakeholders must be involved in an ongoing CIIP dialogue, even across borders (ITAC).

With respect to cross-border co-operation:

- The focus on international co-operation across borders should be maintained. An updated instrument should encourage countries to engage in bilateral and multilateral co-operation to share knowledge and experiences (BIAC).
- CIIP policy should not conflate security with local content or otherwise unduly limit user choice in ICT security products and services, and ensure access to state of the art digital security solutions (BIAC).

With respect to the possibility to update the CIIP Recommendation:

- The CIIP Recommendation should be updated to become consistent with the 2015 Security Risk Recommendation including by supporting a risk management approach (ITAC, CSISAC), and incorporating the principles of responsibility, co-operation, and safeguarding human rights. The Recommendation should encourage collaborative security, support transparency, and preserve the essential properties of the Internet (ITAC). Consistency with the revised Privacy Guidelines, Recommendation on Internet Policy Making Principles and Cancun Declaration should also be sought (CSISAC).
- The CIIP Recommendation continues to be relevant. However, to the extent that modifications are considered, they should encourage member countries to establish non-prescriptive regulatory regimes, foster the growth of collaborative public-private partnerships and voluntary information sharing structures that protect sensitive information, and consider the entire cybersecurity ecosystem, which includes players beyond the traditional communications carriers (BIAC).

Annex D. Questionnaire

Definition/understanding of Critical Information Infrastructures (CII)

In 2008, the OECD defined the concept of CII as follows: "For the purposes of this Recommendation, critical information infrastructures, hereinafter "CII", should be understood as referring to those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy; […]" (Extract from the 2008 Recommendation, available in Annex 1).

1.1. Today, does your government use the concept of Critical Information Infrastructures?

Yes No

– If yes:

1.1.1. What criteria do you apply to identify what is a Critical Information Infrastructure? Please provide a few examples of some of these infrastructures to illustrate your response.

– If no:

1.1.2. What concept do you use in your policy framework (e.g. critical service/sector/operator instead of critical infrastructure) and what is its definition?

1.1.3. What criteria do you apply to define the scope of that policy framework (i.e. identify what is critical)? Please provide examples to illustrate your response.

If you have responded No to question 1.1, please replace the concept of Critical Information Infrastructure in the questions below by the concept you use.

Your country's policy framework and its implementation

General description

1.2. Please provide a general description of your policy framework to protect critical information infrastructures, including references to official documents.[10] Please indicate its scope and overarching objective as well as important legal obligations (e.g. incident reporting, localisation requirement, etc.) and explain their rationale.

1.3. If your policy framework is partially in place, please indicate which elements are in place and which have yet to be developed, adopted and/or implemented.

1.4. If your policy framework is currently evolving or has significantly evolved since 2008, please explain what has changed and why.

Critical Information Infrastructures Protection (CIIP) at domestic level

These questions relate to the implementation of Part I of the Recommendation (in annex) which covers three areas: leadership and commitment, risk management including interdependencies, and partnership with private sector.

Leadership and commitment

1.5. How does your government demonstrate leadership and commitment to protect Critical Information Infrastructures?

1.6. Which government agencies have a responsibility in this area, what are their roles and how does coordination take place?

Risk management, including interdependencies

In your responses to questions 2.6 to 2.9, please feel free to distinguish aspects related to availability, integrity and confidentiality, if this is appropriate.

1.7. How does your national strategy/policy encourage the management of digital security risk to Critical Information Infrastructures?

1.8. Does your policy framework address digital security risk to the information infrastructures that are specific to the operation of critical infrastructures (cf. Figure A D.1, B, green boxes)?

Yes No

– If, yes please describe relevant policy measures (e.g. governance mechanism, regulatory requirement, other measures)?

1.9. Does your policy framework also address digital security risk to critical infrastructures that arise from the use of the general information infrastructures (such as the Internet, public communication networks, etc. Cf. Figure A D.1, C, red boxes)?

Yes No

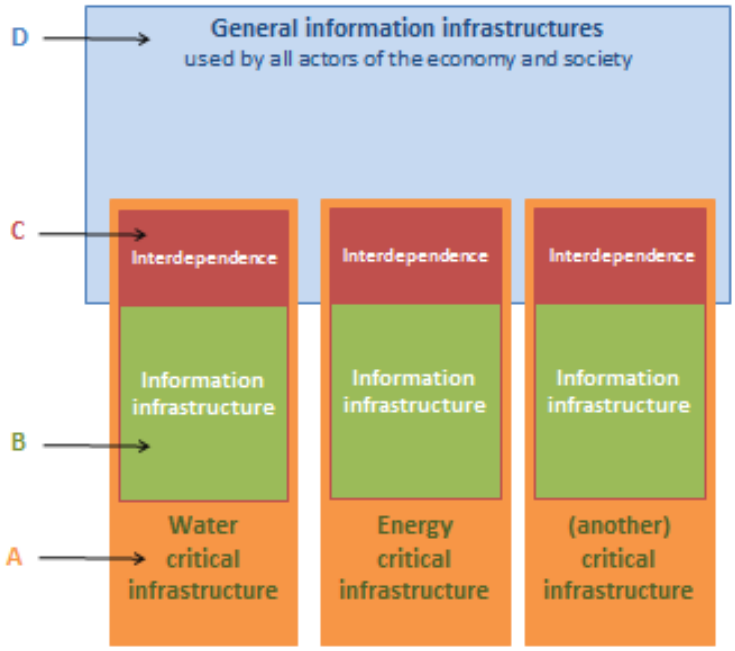
– If, yes please describe relevant policy measures (e.g. governance mechanism, regulatory requirement, other measures)?

1.10. Does your policy framework furthermore address digital security risk to the general information infrastructures used by all actors of the economy and society (e.g. the Internet, parts of it, particular Internet services, etc.) (cf. Figure A D.1, D, blue box)?

Yes No

– If, yes please describe relevant policy measures (e.g. governance mechanism, regulatory requirement, other measures) and indicate which components of the general information infrastructure they address?

Figure A D.1. Interdependencies



Note: This figure aims to illustrate questions Q2.7-Q.2.9. The orange boxes A represent critical infrastructures, taking the water and energy sectors as examples (there are probably other critical infrastructures / sectors, as shown by the third orange box titled "(another) critical infrastructure" which represents them in a generic manner). The green boxes B, addressed in Q2.7, represent information infrastructures that are specific to the operation of each critical infrastructure. The red boxes C, addressed in Q2.8, represent interdependencies, i.e. the part of the general information infrastructures (such as the Internet, public communications networks, etc.) on which critical infrastructures rely. The blue box D, addressed in Q2.9, represents the general information infrastructures used by all actors of the economy and society

1.11. Does your policy framework cover exercises?

Yes No

1.11.1. If yes, please provide details and indicate the purpose of such exercises and how their results are used.

Partnership with the private sector

1.12. How does your government work in partnership with the private sector and other stakeholders? Please indicate what stakeholder groups (e.g. public sector, private sector, civil society, non-governmental organisations) contribute to your country's CIIP policy development, implementation and evaluation and how your government coordinate this input.

CIIP at cross-border level

This question relates to part II of the Recommendation (see annex).

1.13. How does your government work internationally to protect Critical Information Infrastructures across borders?

Review and measurement

1.14. Please describe the processes your government has for reviewing and updating its CIIP policy.

1.15. How do you measure the effectiveness of your policy framework to protect Critical Information Infrastructures?

Please describe the metrics you use, as appropriate.

If statistics can be provided, please do so.

2. Context and drivers underpinning your policy framework

2.1. What are the most significant trends, drivers and challenges related to the protection of Critical Information Infrastructures? Have these evolved since 2008?

2.2. What are the main priorities and goals for your government with respect to the protection of Critical Information Infrastructures? Have they evolved since 2008, and if yes, how? Do you expect them to further evolve over the next 5 to 10 years, and if yes, how?

2.3. What relationship does your government see between CIIP and economic and social development?

2.4. Has a domestic market emerged/developed to address the demand for products and services for the protection of Critical Information Infrastructures?

Yes No

2.4.1. If yes, please describe this trend and indicate what is the role of public policy in the emergence/development of this market.

3. Continued relevance of the 2008 CIIP Recommendation

3.1. Does the OECD concept of Critical Information Infrastructure cover all relevant aspects of what you identify as CII (please see definition above in 1)?

Yes No

3.1.1. If not, what changes are required?

3.2. Should the 2008 CIIP Recommendation be updated to reflect the 2015 *Recommendation on Digital Security Risk Management for Economic and Social Prosperity*, which focuses on risk to the economic and social activities using information infrastructures rather than on the information infrastructures themselves?

Yes No

3.2.1. If yes, please explain why and what changes should be made to the OECD Recommendation. For example, should the focus of the CIIP Recommendation also shift from critical information infrastructure to critical economic and social activities relying on the digital environment?

3.3. What is missing, or should be modified in the 2008 CIIP Recommendation? Please explain why.

3.4. Has your government used the 2008 Recommendation to inform the development of domestic CIIP policies, and if yes, how?

3.5. Does privacy protection need to be addressed in CIIP policy frameworks in the future?

Yes No

3.5.1. If yes, please explain why and, as appropriate, describe current relevant policy measure in your country.

3.6. Please provide any other views or information to help assess the relevance of the CIIP Recommendation today and in the future.

References

ASEAN (2015), *ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies (ICTs)*, 7 May, http://aseanregionalforum.asean.org/files/library/Plan%20of%20Action%20and%20Work%20Plans/ARF%20Work%20Plan%20on%20Security%20of%20and%20in%20the%20Use%20of%20Information%20and%20Communications%20Technologies.pdf

BRICS (2016), *ICT Development Agenda and Action Plan*, 11 November, www.ranepa.ru/images/media/brics/indianpresidency2/11-11-2016%20BRICS%20ICT%20Development%20Agenda%20&%20Action%20plan.pdf

BRICS (2015), *VII BRICS Summit: Ufa Declaration*, 9 July, https://www.brics2017.org/English/Documents/Summit/201701/t20170125_1409.html.

ENISA (2015), *Critical Information Infrastructures Protection approaches in EU*, https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf/view

European Commission (2016), *Directive on Security of Network and Information Systems*, Fact Sheet, http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm

GFCE, Meridian (2016), *The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers*, www.meridianprocess.org/siteassets/tno-jrv161031-02_hr.pdf

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*, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG

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

OECD (2015b), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264229358-en

OECD (2014), *Recommendation of the Council on the Governance of Critical Risks*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/305 http://www.oecd.org/mcm/mcm-2014-chair-summary.htm

OECD (2012), *Cybersecurity Policy Making at a Turning Point*, OECD, Paris, http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

OECD (2008), *Recommendation of the Council on the Protection of Critical Information Infrastructures*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/121

OECD (2007), *Development of Policies for the Protection of Critical Information Infrastructures*. OECD, Paris, www.oecd.org/sti/40761118.pdf

OECD (2002), *Recommendation of the Council concerning Guidelines on the Security of Information Systems and Networks: Towards a Culture of Security*, OECD, Paris, www.oecd.org/sti/ieconomy/15582260.pdf

Petit F. et al (2015), *Analysis of Critical Infrastructure Dependencies and Interdependencies*, Risk and Infrastructure Science Centre, Argonne Laboratory. http://www.ipd.anl.gov/anlpubs/2015/06/111906.pdf

Rinaldi, S.M., J.P. Peerenboom and T.K. Kelly (2001) *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*. IEEE Control Systems, 21, 11-25, http://dx.doi.org/10.1109/37.969131

Setola R., and M. Theocharidou (2016) "Modelling Dependencies Between Critical Infrastructures". In: Setola R., V. Rosato, E. Kyriakides and E. Rome (eds.) *Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control*, vol 90. Springer, Cham https://doi.org/10.1007/978-3-319-51043-9_2

Wenger A., Metzger J., Dunn M. (2002), *International CIIP Handbook*. ETH Zurich, www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP_Handbook_2002.pdf

NOTES

[1] Then called Committee on Information, Computer and Communications Policy (ICCP).

[2] Belgium, Canada, Chile, Colombia, Czech Republic, Estonia, France, Germany, Japan, Korea, Norway, Poland, Russia, Spain, Sweden, Turkey, the United Kingdom and the United States.

[3] Most recommendations are updated by developing a new Recommendation that replaces the old one.

[4] The Business and Industry Advisory Committee to the OECD (BIAC), Civil Society Internet Society Advisory Council (CSISAC) and the Internet Technical Advisory Committee (ITAC).

[5] According to the OECD 2007 report on the *Development of Policies for the Protection of Critical Information Infrastructures*, the concept of CII appeared in the early 2000s as "a somewhat neutral and general term in the international community" that was not commonly used in national public policy frameworks and did not have at the time a commonly agreed definition. Moreover, the analysis underlined that the diversity of policies in the seven countries compared did not allow for a single common formal definition of CII to emerge from the work. Instead, the study introduced a "common understanding" of the concept, "broad enough to accommodate the different national needs and approaches". This common understanding was later inserted in the CIIP Recommendation (Box A A.2) as a first step designed to increase policy awareness on this emerging subject rather than as a mature concept based on experience

[6] Keeping in mind that the OECD 2015 Security Risk Recommendation defines risk as the "effect of uncertainty on objectives", building on ISO/IEC 31000 and 27001. Cf. (OECD, 2015a, p. 31[5]).

[7] "Data have no intrinsic value; their value depends on the context of their use", p. 197.

[8] Each observation does not necessarily reflect the views of more than one country. Some of these observations may be related to cultures and styles of government.

[9] See for example article 5.2.a of the Directive.

[10] E.g. titles and dates of policy texts, laws and regulations, attachments or hyperlinks to official documents if possible in English or French.