Best Practices for Critical Information Infrastructure Protection (CIIP)

Experiences from Latin America and the Caribbean and Selected Countries

Authors:
Antonio García Zaballos
Inkyung Jeun

KISA
IDB

Best Practices for Critical Information Infrastructure Protection (CIIP)

Experiences from Latin America and the Caribbean and Selected Countries

Authors:
Antonio García Zaballos
Inkyung Jeun

KISA IDB

Cataloging-in-Publication data provided by the
Inter-American Development Bank
Felipe Herrera Library

García Zaballos, Antonio. Best practices for Critical Information Infrastructure Protection (CIIP): experiences from Latin America and the Caribbean and selected countries / Antonio García Zaballos and Inkyung Jeun.

p. cm.
Includes bibliographic references.

1. Computer networks-Security measures-Latin America. 2. Computer networks-Security measures-Caribbean Area. 3. Information networks-Security measures-Latin America. 4. Information networks-Security measures-Caribbean Area. 5. Data protection-Latin America. 6. Data protection-Caribbean Area. I. Inkyung, Jeun. II. Inter-American Development Bank. Capital Markets and Financial Institutions Division. III. Korea Internet & Security Agency. IV. Title.
IDB-CP-44

Publication Code: IDB-CP-44
JEL Codes: O3, O38
Keywords: broadband, critical information infrastructure protection, cyber attack, security

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Inter-American Development Bank, its Board of Directors, or the countries they represent, or of the KISA.

The Inter-American Development Bank and the KISA do not guarantee the accuracy of the data included in this work.

Inter-American Development Bank
1300 New York Avenue, N.W.
Washington, D.C. 20577
www.iadb.org

The Institutions for Development Sector was responsible for the production of this publication.
External Vendors:
Production Editor: *Sarah Schineller (A&S Information Specialists, LLC)*
Editor: *Sheila Mahoney*
Design: *Word Express, Inc.*
Proofreader: *Sue Debowski*

Table of Contents

List of Figures

List of Tables

List of Boxes

List of Acronyms

API	Application Program Interface
CERT	Computer Emergency Response Team
CERT-CC	CERT Coordination Center
CI	critical infrastructures
CII	critical information infrastructure
CIIP	critical information infrastructure protection
CIP	critical infrastructure protection
CNI	critical national infrastructure
CNPIC	National Center for the Protection of Critical Infrastructure, Spain
CPII	Committee for the Protection of Information Infrastructure
CPNI	Centre for the Protection of National Infrastructure, UK
CSIRT	computer security incident response team
DG HOME	Directorate General for Migration and Home Affairs, European Commission
DG ECHO	Directorate General for Humanitarian Aid and Civil Protection, European Commission
DHS	Department of Homeland Security, United States
EC	European Commission
ECI	European Critical Infrastructures
EPCIP	European Programme for Critical Infrastructure Protection
FBI	Federal Bureau of Investigation
FDI	foreign direct investments
FICORA	Finnish Communications Regulatory Authority, Finland
IDB	Inter-American Development Bank
ICIC	National Program for Critical Information and Cybersecurity Infrastructure, Argentina
ICT	information and communications technology
IT	information technology
JRC	Joint Research Center
KISA	Korea Internet & Security Agency
Korea	Republic of South Korea
LAC	Latin America and the Caribbean
MSIP	Ministry of Science, ICT and Future Planning, Korea
NATO	North Atlantic Treaty Organization
NCIPA	National CIP dedicated Agency
NESA	National Emergency Supply Agency, Finland
NESC	National Emergency Supply Council
NESO	National Emergency Supply Organization, Finland
NIPP	National Infrastructure Protection Plan
NIS	National Intelligence Service
NISAC	National Infrastructure Simulation and Analysis Center
NRA	National Risk Assessment
NRR	National Risks Register
NSRA	National Security Risk Assessment
ONTI	National Office of Information Technologies

PPD	Presidential Policy Directive
PPP	Public-Private Partnership
PSN	National Security Program
SCADA	Supervisory Control And Data Acquisition
SLA	Service level agreements
SLO	Security Liaison Officers
SLTT	state, local, tribal, territorial
SSA	sector-specific agency
Subtel	Subsecretary of Telecommunications of Chile
TLP	Traffic Light Protocol
TNCEIP	Thematic Network on Critical Energy Infrastructure Protection
UK	United Kingdom
WDR2014	World Development Report 2014
WEF	World Economic Forum

About the Authors and Contributing Organizations

Antonio García Zaballos is a lead specialist on telecommunications in the Institutions for Development Division of the Inter-American Development Bank (IDB). He is also the leader of the broadband initiative. He has extensive experience in the telecom sector, where has worked in a variety of different positions at increasing levels of responsibility. At Deloitte Spain, he led regulation and strategy for Latin America and the Caribbean, and previously he was the chief economist of the Cabinet for Economic Studies of Regulation at Telefónica of Spain. Before joining Telefonica, Antonio was deputy director of economic analysis and markets at the Spanish telecom regulator. During his career, Antonio has provided advisory services to regulators, telecom operators, and governments in countries such as Argentina, China, the Czech Republic, the Dominican Republic, Ecuador, Paraguay, Polonia, and Saudi Arabia. He holds a PhD in economics from the University Carlos III of Madrid and is an associate professor of applied finance for telecommunications at the Instituto de Empresa business school. He is the author of several publications on economics and regulations in the telecommunications sector.

Inkyung Jeun is a consultant with the Capital Markets and Financial Institutions Division of the IDB. Prior to joining the Bank, she was manager of the Computer Emergency Response Team at the Korea Internet and Security Agency. Before she joined that agency, she was a researcher at Samsung Electronics Co. She holds a PhD in computer engineering from Sungkyunkwan University in South Korea, where she studied cyber security, cryptography, authentication, and privacy. She is a Certified Information System Security Professional and a Certified Information System Auditor.

The Inter-American Development Bank (IDB) supports efforts by Latin American and Caribbean countries to reduce poverty and inequality. It aims to bring about development in a sustainable and environmentally friendly way. The IDB is the largest source of development financing for the Latin American and Caribbean region, with a strong commitment to achieve measurable results and increase integrity, transparency, and accountability. It has an evolving reform agenda that seeks to increase its development impact in the region. The IDB provides loans, grants, and technical assistance, and develops research. Its membership includes 48 shareholding countries, 26 of which are in the Latin American and Caribbean region.

The Korea Internet & Security Agency (KISA) is performing one of the urgent tasks of our time—improving the global competitiveness of Korea's internet industry. It has set internet promotion for the future and information security for our safety as its primary tasks. The agency is focusing on enhancing the information security capacity of Korea's ICT industry and expanding global cooperative partnerships based on the K-ICT Security Development Strategy. The goal is for these twin pillars to serve as the core competencies of the future Korea in equal and harmonious measure. Based on these efforts, the agency aims to reaffirm Korea's position as a future internet powerhouse armed with global competitiveness and to lead the Korean economy in making another leap forward through intensive promotion of the ICT industry.

Acknowledgments

This publication was made possible with the support from the Knowledge Partnership Korea Fund for Technology and Innovation, established with a contribution from the Government of the Republic of Korea. The authors would like to recognize Logical Standard, which produced the initial report for this publication; Sheila Mahoney, who copyedited the manuscript; and Sarah Schineller, who was responsible for the editorial and production process. We are particularly grateful to Natalija Gelvanovska who acted as external peer reviewer and provided useful suggestions to improve the original draft. A special thank you goes to Phil Keefer, who enriched the final draft with very useful comments.

Executive Summary

Over the past few decades, Latin America and the Caribbean (LAC) has witnessed numerous changes in its development, with most being beneficial. Notwithstanding considerable variation, most countries experienced technological modernization and economic growth. Positive changes relate to sizable growth and expansion of the region's network infrastructure sectors, such as transport, energy, and information and communications technologies (ICT), among others. Modernization and expansion revealed old and brought new risks that arose from the widespread reliance on infrastructure assets and systems as well as from increasing interconnectivity of different structures on the national and international levels. If ignored, those risks could turn into large-scale disruptions of infrastructure, resulting in significant impact on the population and vital functions of society. Infrastructures that could provoke such impacts and possibly cascading effects are known as critical infrastructures. In many cases, ICT interconnects these critical infrastructures, creating substructures referred to as critical information infrastructures (CIIs). CIIs are an important part of critical infrastructures because they are the telecommunications backbone and the uninterrupted exchange of data is essential to the operation of infrastructures and the services that they provide. Hence, critical infrastructures and CIIs will not be discussed as completely separate concepts in this publication, rather they will be referred to as critical infrastructures.

The reality is that, despite risks, modern society cannot evolve and operate without relying on critical infrastructures. Furthermore critical infrastructures perform numerous vital functions without which today's life would be inconceivable, such as energy supply, water and sanitation networks, financial services, and mobile and fixed communications. It is thus not a matter of choice, but of a strategic approach to how to manage the risks, and identify and protect national critical infrastructures. This study was commissioned at an important moment—when LAC is entering an accelerated path of infrastructure expansion and modernization. This publication is written to provide insights to the strategic thinking behind the creation of the national critical information infrastructure protection (CIIP) frameworks. It also builds its recommendations on in-depth analysis of the best CIIP practices around the world, with consideration of the region-specific landscape to originate a base line from which further development can be delineated.

The European Union (EU, as a region), Finland, Republic of South Korea (Korea), Spain, United Kingdom (UK), and the United States were chosen as case studies for this publication. Selection criteria for case studies included risks, challenges, and specific experiences faced by the countries; geographical variety; and maturity of the CIIP frameworks. The authors decided to look at the EU as a unique example of regional CIIP coordination that may be worth considering in the LAC region. The

EU's CIIP framework enables region-wide coordination and a response framework for large-scale cross-border disruptions.

The structure of this publication mirrors a typical structure for a CIIP framework, which comprises the following pillars:

- Strategy and legislation
- Governance and regulation
- Definition and assignment
- Protection
- Information sharing
- Crisis management

Case studies provide focused input into each pillar and are thus spread through the publication. The reader may observe a number of similarities, but also differences, among case studies. Studied approaches ultimately emerge around the core understanding of the vitality of the CIIP agenda. Many identified critical infrastructures are similar among the different countries and pillars of different CIIP frameworks are alike. In turn, implementation details vary depending on the national circumstances (risks), institutional structure, governance framework, and cooperation practices. Granular analysis of different CIIP frameworks allowed the authors to highlight the strengths and successes achieved by individual countries or regions and thus formulate best practices and lessons learned. The authors believe that experience and advances in CIIP could encourage LAC countries to benefit from such expertise to secure more robust and sustainable economic growth.

Beyond analysis of the international case studies, the value added of this publication is its authentic region-wide research on the critical infrastructure protection (CIP) landscape in LAC. The investigation covered both public and private sectors in 26 countries and comprised desk research, electronic surveys, and follow-up interviews. Electronic surveys were sent to over 900 private and public sector representatives that were identified in advance. This challenging exercise allowed the authors to collect a statistically representative sample, with a 13.9 percent response rate for the region. Though the overall response rate could be considered low, it should not be underestimated because CIP is a sensitive topic and public institutions and private companies are reluctant to share any type of information. However, it may also be indicative of lower awareness about CIP, and CIIP even more so. The authors chose to focus on CIP instead of CIIP to improve the inclusiveness of the topic and improve survey participant response results.

In terms of the response rate, all 26 countries participated in the survey, providing from 1 to 12 responses, with an average rate per country of approximately 5 responses. The public sector was more responsive to the survey; the number of responses from critical infrastructure operators surpassed the total from public agencies in only 7 of 26 countries. The most responsive participants were public agencies and public companies in the ICT, energy, and finance sectors. As is typical of large-scale surveys, the accuracy of this research is not absolute and information submitted should not be treated as fact reflecting the actual situation with regards to CIP at the country level. Results of this research were aggregated using empirical and statistical methods. To achieve higher accuracy and precision at the country level, the research would have to be complimented with on-site visits in individual countries; face-to-face interviews with CIP-related bodies, companies, and local experts; and exercises measuring CIP effectiveness.

Overall CIP and CIIP issues appear to be relevant to both private agencies and private companies in the LAC region. This is not surprising considering 54 percent of LAC countries reportedly experienced large-scale disruption of critical infrastructure in the past five years. In terms of feedback on CIP awareness and CIP framework development, analysis revealed disparities between the individual countries. At the national level, the surveys also showed inconsistency in awareness about the national CIP policy since participating agencies and companies sometimes provided contradictory answers regarding the same aspects of CIP framework development and implementation.

Overall, the results of the survey indicated a good level of strategic CIP guidance, but a lower level of adoption of CIP-related legislation. Indeed, 42 percent of LAC countries have adopted CIP strategies or integrated CIP elements in the national security strategies. However, primary CIP legislation was only adopted in 27 percent of LAC countries and only 15 percent have secondary legislation where critical infrastructure is directly addressed. Only 35 percent of LAC countries have a dedicated government institution responsible for CIP. Results indicate a gap between government initiatives (policy) and common political agreement to adopt a CIP framework (legislation). Therefore, this linkage needs to be strengthened to foster implementation of the CIP agenda.

Those countries that have adopted CIP policies most commonly include transport, energy, government, healthcare, ICT, emergency services, and water as critical sectors, which is in line with international practice. Analysis of the questionnaire results confirmed that, when compared to public agencies, critical infrastructure operators are better prepared in terms of crisis management, but are less aware of the CIP policies and coordination procedures. The majority (65 percent) of LAC countries report cooperation with the private sector is in place. This is a very positive indication that CIP could improve in the future. However, consistent national coordination and systematic information exchange are well established in only a few countries. Therefore, the capacity of the critical infrastructure operators needs to be increased regarding national CIP priorities and policy approaches. Establishment of national and sectoral CIP groups may be an efficient way to address the situation.

Analysis of the responses allowed for a fairly accurate clustering of the LAC countries into four groups or stages based on pre-identified criteria related to CIP framework development. This exercise was performed to allow the authors to adjust recommendations that were derived from the analysis of international best practices. Thus each recommendation is rated for its relevance for each of the clusters. Clustering criteria were designed considering this is the first region-wide study targeting CIP framework in a comprehensive manner. CIP and CIIP are mostly new to the region, so the overall objective of this exercise was to establish a baseline. If this exercise becomes regular, greater participation rates and progress tracking would be expected. Also of note, information related to national CIP frameworks is not always publicly available in full and therefore details cannot always be collected.

According to the information collected through the survey, countries were grouped into four stages taking into account two criteria: level of CIP framework and governance development; and critical infrastructure identification practices. Clustering results (Table 6.4 and Figure 6.12, page 87) revealed that the majority of countries (17) with different levels have undertaken steps toward developing a CIP framework and establishing a governance model. However, nearly half of the countries (16) still need to undertake efforts in CIP, such as systematically identifying critical infrastructure sectors and cataloguing critical infrastructure assets within each sector; working with the private sector to define and put in place protective measures and procedures. Recommendations of this study were specifically designed to support development of the CIP framework and governance model and to provide practical insights into protecting critical infrastructures. All recommendations are derived from specific examples found across the reviewed international practices.

The authors note that ours is not an ideal world and many risks materialize before systems are fully ready. As the review of the case study countries proved, many CIIP initiatives and improvements were, unfortunately, triggered not by advance work or extensive studies, but by emergency situations, many of which had catastrophic consequences. No CIIP framework was developed in perfect sequence and exactly following the prescribed steps. It is also unlikely that any CIIP framework ever would. Nonetheless, countries should continue to strive for perfection even though life will introduce its own adjustments to this process. The most important lesson to be learned is that any effort performed in advance to strengthen CIIP can make a great change in terms of human lives and economic consequences.

The introduction to this publication provides the overall reasoning and relevance of the topic to the region. Chapter 2 reviews CIIP framework development and governance models across selected international cases and concludes with lessons learned and takeaways. Chapters 3 to 5 focus on practical aspects of identifying and protecting critical infrastructures, building recommendations on the practices applied across international cases. Chapter 6 provides an overview of the survey methodology and highlights some conclusions from the replies submitted by the private and public sectors in the region. It also provides the results of the clustering exercise for the LAC countries. Chapter 7 provides a consolidated list of recommendations, rating the relevance of each for different groups of countries. Additional case studies of five countries in the LAC region (Argentina, Bolivia, Chile, Costa Rica, and Mexico) are provided in the appendices for comparison.

1

Introduction to CIIP

Infrastructure is usually referred to as the basic physical and organizational structure required for a society to operate. Currently, although there is no unique or standardized definition of this term, the concept of infrastructure could be divided into economic infrastructure, social infrastructure, and soft infrastructure (Alberti, 2015). The World Economic Forum (WEF) defines economic infrastructure as a composition of transport facilities (air, sea, and land), utilities (water, gas, and electricity), flood defenses, and waste management, among other facilities and services (WEF, 2012). There is indisputable evidence that economic infrastructure expansion and economic growth are closely related (Calderon and Serven, 2010).

Infrastructure enhancement promotes growth, equity, and environmental sustainability. The Inter-American Development Bank (IDB) is one of the major donors to the Latin American and Caribbean (LAC) region. The Bank supports the achievement of sustainable social and economic progress. Thus, a considerable portion of the IDB's loan portfolio is dedicated to infrastructure financing, such as energy, transport, and water and sanitation (Box 1.1). Other donors active in the region, such as the World Bank, the Development Bank of Latin America, and the United Nations Conference on Trade and Development, are following a similar approach. Yet, the region is lagging and needs to catch up within a number of infrastructure advancement parameters. Infrastructure expansion is thus unavoidable and essential to underpin future economic growth. Nearly 600 million people populating 26 LAC countries will increasingly rely on new and existing infrastructure.

Infrastructures of significant national importance are being referred to as critical infrastructures. Modern societies rely heavily on critical infrastructures such as electricity, gas, financial institutions, and information technology (IT) to perform day-to-day activities and implement future growth strategies. In many countries and across different regions, the topic of critical information infrastructure protection (CIIP) attracts increasing attention of policymakers. It is progressively considered an integral part of national sustainability strategies since a large-scale disruption of critical infrastructures can have cascading effects and impact a large part of the population and vital functions of society.

Furthermore, higher attention to CIIP enables improved conditions for doing business in developing countries. Indeed, as far as needs of the business community are concerned, "prolonged neglect of critical infrastructure and its development needs" is ranked fourth among major concerns in emerging markets and developing economies for business stimulation, economic integration, and trade performance (WEF, 2015). The first three concerns are related to fiscal and liquidity crises. Unfortunately, according to the findings of the WEF, in the past 10 years little progress has been made in addressing the risk of failure of critical infrastructures.

There are two major trends that are expected to have considerable impact on CIIP approaches

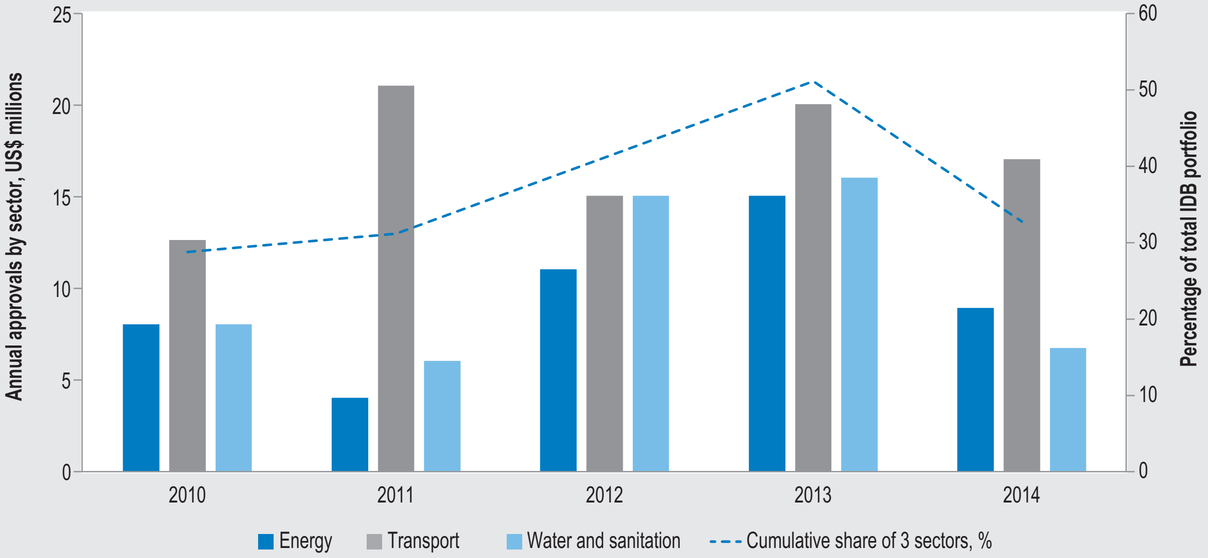
Box 1.1. Multilateral Organizations Support Infrastructure Investments

Hard infrastructure projects (e.g., transport, energy, and water) that are traditionally defined as critical infrastructure are also long-standing lending priorities for international multilateral institutions, including major investors in the region such as the IDB and World Bank.

In 2010, the IDB approved $3.6 billion in loans for transport, energy, and water and sanitation infrastructure. In 2014, this number grew to $4.6 billion. Over the 2010–14 period, the share of the IDB's lending portfolio for those three infrastructures was on average 36 percent (see Fig. 1.1).

Similarly, during 2011–14, the World Bank's annual global investments in those three sectors constituted about 40 percent of its entire portfolio. Of note, the World Bank includes flood prevention in the water and sanitation sector and includes mining in the energy sector.

FIGURE 1.1. Annual IDB Lending to Transport, Energy, and Water and Sanitation Sectors, 2010–14



Source: Authors based on IDB 2010–14 annual reports and the World Bank 2014 annual report.

in LAC: urbanization and digitalization of infrastructures. The high concentration of the population in urban centers implies greater reliance on critical infrastructures and more significant implications of disruptions. The second trend is not specific to LAC and is related to technological modernization of economic infrastructures. Advanced IT allow greater efficiencies in terms of operation costs, and new functions and services for its operators and end users. Today nearly all new infrastructure investments incorporate a "smart" component as part of the project, such as process control systems[1] and automation technology. Among such examples are smart (electric) grids and intelligent transport systems (Box 1.2). This trend creates new risks related to cyber threats to which all IT systems and networks are susceptible.

Specifically, technological advances have created substructures within critical infrastructures, which are usually referred to as critical information infrastructures (CII) (Box 1.3). It is important to

[1] For example, process control systems used by the energy utility industry to control and monitor the generation, transmission, storage, and distribution of electric power, gas, and heat in combination with controlling the supporting processes, ISO/IEC TR 27019:2013.

Box 1.2. Urbanization Is Putting Pressure on Infrastructure Efficiency and Resilience

Urbanization is one of the key trends not only in LAC, but also globally. According to Dobbs et al. (2011), the global urban population has been rising by an average of 65 million people annually during the past three decades, the equivalent of adding seven cities the size of Chicago a per year, every year. Among others, the LAC region could be deservedly named the world's urban leader. Indeed, in 1950, only 40 percent of the population lived in urban areas in LAC. In 1990, that number had increased to 70 percent and, in 2013, to 79 percent.[a] UN Habitat estimates that, in 2050, 90 percent of LAC's population will be urban.

Concentration of the population in urban areas raises many issues related to sustainable development. Reliability and robustness requirements for urban infrastructure are among the challenges, as they become increasingly critical for highly concentrated urban citizens. Protecting critical infrastructures within cities thus deserves special attention within the national critical infrastructure protection (CIP) frameworks in LAC.

Consider, for example, urban transportation infrastructure, which must fulfill more than one role at a time: driver aids, fare collection, traveller information, traffic monitoring, security (including surveillance of vehicles, stations, running-way, public transport infrastructure, and facilities), demand-responsive transport, etc. Interruption of such a system in a big city could cause chaos. Similarly, a disruption of the urban energy distribution systems would trigger serious disorder.

In the LAC region, transport projects that include elements of intelligent transport systems are only just gaining a presence. These systems are being integrated into surface transportation systems on a project-by-project basis and, nationwide, their architectures are still rare. However, over time, the natural pace of development of many critical infrastructure sectors foresees technological evolution toward smart systems. In this context, the region has time to incorporate CIIP measures from the very beginning, which is far more efficient than doing it later.

Sources: Arsht (2014); Dobbs, Manyika, and Woetzel (2015); Dobbs et al. (2011).

[a] *See http:*//data.worldbank.org/indicator/SP.URB.TOTL.IN.ZS.

Box 1.3. Critical Infrastructure and Critical Information Infrastructure

Critical infrastructure and critical information infrastructure (CII) are different but linked. However, the link is largely being overlooked. For the purpose of this publication, which addresses critical infrastructures in general, it is important to distinguish between the two. Critical infrastructures include but are not limited to CII, thus CII is critical infrastructure, but not all critical infrastructures are CII. Failure of CII may lead to failure of critical infrastructure, but critical infrastructure may fail for many other reasons in no way related to CII. For instance, critical infrastructure could fail as a result of a natural catastrophe like an earthquake or flood, while failure of CII is mainly caused by cyber-related threats (i.e., cyber-attacks) or by failure of a critical infrastructure. This implies that critical infrastructure is more susceptible to a broader variety of risks than CII.

As a consequence of critical infrastructure protection (CIP) policies, regulations are addressing a much broader and more comprehensive set of risks, including, but also far beyond, CII-related risks. Protection of CII is much more focused on technology.

Consequently, risks attributed to failures of critical infrastructure and failures of CII are usually being perceived differently. For instance, the WEF (2015), in its annual *Global Risk* report, considers failure of critical infrastructure an economic risk, while failure of CII is technological. In the 2015 edition of the report, the scores for the likelihood parameter were comparable for both; however, the risk of CII breakdown was perceived to have twice the impact of a failure of critical infrastructure. This result may partially be attributed to currently greater awareness of threats related to cyber security.

Source: Authors; WEF (2015).

Box 1.4. ICT and Foreign Direct Investments, 2013–14

In 2013, the ICT sector was identified as the fastest growing sector for FDI globally. In 2013, ICT and internet infrastructure activity attracted $48.7 billion of the $61.6 billion invested in the sector globally, which appears to correspond with the growth of subsectors that all require high levels of infrastructure deployment. The capital spent on ICT and internet infrastructure in 2013 was the highest recorded since FDI markets began tracking the data. In LAC, the ICT sector accounted for $17.0 billion of capital investments and was the second biggest sector in terms FDI in 2013.

As a part of data and voice communications infrastructure, there is rising demand for cloud storage and data back-up infrastructure, which forms an important part of CII. Not surprisingly, despite an overall decrease in FDI growth, from 11 percent in 2013 to 1 percent in 2014, capital investments in data centers have been on the rise since 2009, both in terms of capital investments and number of projects. Globally, between 2009 and 2014, data center FDI increased on average 12 percent year-over-year for projects and 3.5 percent for capital investments. So far, LAC countries are not among the top destinations for data center FDI. However, there are important preconditions for that in the future. For instance, software and IT services in LAC accounted for the largest number of FDI projects, at 121, despite a fall of 18 percent compared with 2013.

Source: Authors and fDi Intelligence (2014; 2015).

distinguish between them and to keep in mind that neither should be addressed in isolation from the other. This study addresses CIIP, and for the purpose of this publication, the term critical infrastructures includes CIIs.

There are a number of reasons CIIP deserves significant attention. Not only are elements of CII penetrating traditional critical infrastructures, but also CII could be seen as a standalone critical infrastructure. Examples include elements of information and communications technology (ICT) and ICT systems such as internet connectivity and telephony communications networks. The complexity of CIIP derives from its decentralization in terms of geographical location and ownership. Of all the traditional critical infrastructure sectors, ICT is perhaps the one attracting the most participation from private capital, including significant foreign direct investments (FDI) (Box 1.4). Therefore, CIIP frameworks for CII ultimately rely on public–private cooperation and information sharing. The LAC region is not an exception, as investments in ICT are expected to increase with the overall growth of ICT markets in the region.

Selection of Case Studies

Currently, a number of countries have acknowledged the significance of CIIP by enacting relevant policies and regulations. However, the majority of nations are only starting to recognize the importance of CIIP. The objective of this section is to review the policy and legal measures for CIIP in selected countries and regions to start the process of developing best practices and formulating lessons learned. This section discusses in detail the CIIP approaches in the EU as a region and in five countries: Finland, Korea, Spain, the UK, and the United States.

The EU region was selected as a unique example of a regionally coordinated CIIP framework. Region-wide CIIP coordination reveals a number of advantages that may be beneficial for LAC. Examples of EU member states were also reviewed (Finland, Spain, and the UK) to showcase deviations in the advancement of national CIIP strategies, taking into account national specifics and also differences in implementing the EU CIIP framework.

Among the criteria for selection as a case study were the maturity of CIIP and the level of know-how accumulated over time. Spain, the UK, and the United States were selected based on long and outstanding experiences at the national level, where CIIP considerations were affecting national policies and legal framework starting from the last century. Spain's case was also included because of the country's close economic and social relationship with the LAC region.

High dependency on modern technologies was another selection factor. Finland and Korea were selected because of outstanding ICT sector environments and high reliance on modern technologies. Those experiences will become increasingly important for the LAC region, as more technological advances will be introduced across different critical infrastructure sectors.

Additionally, the set of countries selected represents different geographic regions and includes countries of different sizes. All these variations allow readers to appreciate different aspects of CIIP and measures put in place. Lastly, case studies of five LAC countries (Argentina, Bolivia, Chile, Costa Rica, and Mexico) are provided for reference in the appendices.

2

Policy and Governance in Selected Countries

Why Is a Critical Infrastructure Information Protection Policy Needed?

The concept of critical infrastructure information protection (CIIP) is not new. Safeguarding strategic national resources and assets has been part of national defense planning since World War II and throughout and after the Cold War. However, modern realities have had a significant impact on governments' perception of CIIP and the ways it is being addressed. The change in perception is motivated by (1) **security** concerns, (2) long-term **development** objectives, and (3) **financial** considerations. Because of these considerations, countries are trying to identify and protect their critical assets against a variety of threats. The starting point is a coherent policy and legal environment. This chapter is dedicated to policy, legal, and regulatory approaches in the countries selected as case studies. The authors also review adopted governance frameworks and summarize the experiences of the countries. First, the authors briefly discuss the three motivations for CIIP.

Security

Society, businesses, and politics depend on well-functioning critical infrastructures. An important task of preventive security policy is to safeguard facilities of major importance to the community whose failure or disruption would cause a long-term shortage of supplies, significant disruptions to public order, or other dramatic consequences. The terrorist attacks in New York City and Washington, DC, on September 11, 2001, in Madrid in 2004, and in London in 2005 are some examples related to risks and vulnerabilities from people. However, infrastructures are being threatened not only by terrorist attacks, but also natural disasters such as the Japanese earthquake and tsunami in 2011, which caused a Level 7 nuclear meltdown at the Fukushima Daiichi Nuclear Power Plant, as well as other types of serious accidents, breakdowns, and system errors.

Development

Beyond security, long-term development policy relies on the integrity of critical infrastructures. Not surprisingly, the *World Development Report 2014* (World Bank, 2014) was dedicated to managing risks. The report argued that a risk-based approach to policy planning could be a powerful tool for development as well as for critical infrastructures since the resilience and robustness of infrastructure are important preconditions for national advancement (Box 2.1). Even though the report was not dedicated to analyzing specific risks, it provided powerful advice on risk management frameworks that could be used by governments, including for the purpose of CIIP.

Box 2.1. Insights into Risk Management from the World Development Report 2014

In 2014, the World Bank's annual flagship publication (World Bank, 2014), was dedicated to development risks. It argued that risk management can be a powerful instrument for development, not only by building people's resilience and thus reducing the effects of adverse events, but also by allowing them to take advantage of opportunities for improvement.

The following were five important insights of risk management from the report:

1. Taking on risks is necessary to pursue opportunities for development. The risk of inaction may well be the worst option of all.
2. To confront risk successfully, it is essential to shift from unplanned and ad hoc responses when crises occur to proactive, systematic, and integrated risk management.
3. Identifying risks is not enough. The trade-offs and obstacles to risk management must also be identified, prioritized, and addressed through private and public action.
4. For risks beyond the means of individuals to handle alone, risk management requires shared action and responsibility at different levels of society, from the household to the international community.
5. Governments have a critical role in managing systemic risks, providing an enabling environment for shared action and responsibility, and channeling direct support to vulnerable people.

Source: Authors based on World Bank (2014).

Financial

The financial losses due to critical infrastructure failures are significant and impact both the public and private sectors. Without proper policy to address CIIP, a country's costs of doing business could rise significantly. For instance, in September 2003, an electrical blackout in Italy (Jonkeren et al., 2012) affected the whole country, cutting off the energy supply to approximately 45 million people. Electricity was not supplied for between 1.5 and 18 hours in different regions of the country. Economic analysis of the negative impact of the breakdown in one critical infrastructure (electricity) to the interlinked industries showed that the full system of 56 industries at the national level resulted in economic losses of €81.79 million for the 11 critical infrastructure industries (those with the highest interdependency) and €123.17 million for all 56 industries combined (Jonkeren, et al., 2012). Moreover, the authors estimated that the cost of 24 hours of downtime as a result of a cyber-attack on a critical infrastructure averages US$6 million per day (Hämmerli and Renda, 2010). The estimated cost of cyber-attacks was thought to be $1.75 billion yearly, but this estimate does not take into account the opportunity cost to businesses that experience loss of service. According to an Organization for Economic Co-operation and Development report on malicious software, the estimated annual loss to U.S. businesses caused by malware is US$67.2 billion (OECD, 2008). Thus, CIIP is first and foremost a matter of national interest and responsibility. The following sections organize and outline good practices in CIIP policy.

CIIP Policy and Governance in the European Union

Strategy and Legislation

Threats to the economic and social wellbeing of citizens were major drivers for the creation of the European Union (EU) critical infrastructure protection (CIP) framework and a number of disruptive events led to its strengthening.

The EU is an economic and political partnership between 28 European countries based on the

TABLE 2.1. Key Policy and Legal Documents Forming the EU's CIIP Framework

Year	Title	Objective
2003	A Secure Europe in a Better World— European Security Strategy, December 12, 2003 (EU, 2003)	Defines the EU's security environment and identifies key security challenges and subsequent political implications for the EU. Provides the conceptual framework for the Common Security and Defense Policy.
2004	European Programme for Critical Infrastructure Protection (EPCIP) (EC, 2004)	High level document establishing the basic CIP pillars for the EU.
2006	Communication from the Commission on the EPCIP 12.12.2006 COM(2006) 786 final (EC, 2006)	Explanatory document to facilitate transposition of the EPCIP at the national level.
2008	Directive 2008/114 to identify and designate European critical infrastructures and evaluate the need to protect them (EU, 2006)	Mandates principles and procedures to delineate critical infrastructure at the EU level, or the national critical infrastructure that is recognized as critical infrastructure on the EU level.
2010	The Stockholm Programme—An Open and Secure Europe Serving and Protecting Citizens, 2010/C 115/01 (EU, 2010)	Formulates a roadmap for EU work for justice, freedom, and security.
2010	Communication from the Commission to the European Parliament and the Council on the EU Internal Security Strategy in Action: Five Steps Towards a More Secure Europe, 22.11.2010 COM(2010) 673 final (EC, 2010a)	Identifies and tackles common EU security threats, such as national disasters, criminal networks, and radicalization.
Supporting documents		
2012	Commission Staff Working Document on the Review of the EPCIP SWD(2012) 190 final (EC, 2012a)	Summarizes the results of the review of the EPCIP and CIP Directive.
2013	Commission staff working document on a new approach to the EPCIP, 28.8.2013 SWD (2013) 318 final (EC, 2013)	Institutes a new approach for the EPCIP organized around three pillars: prevention, preparedness, and response.

Source: Authors.

rule of law: everything that it does is founded on EU treaties (EU, 2012) voluntarily and democratically agreed to by all member states. In the EU, critical infrastructure has been defined (EU, 2008) as an asset or system that is essential to maintain vital societal functions. Damage to, destruction of, or disruption of a critical infrastructure by natural disaster, terrorism, criminal activity, or malicious behavior may have a significant negative impact on the security of the EU and the wellbeing of its citizens.

As a result of that common understanding among all the member states, the EU has developed a set of documents (Table 2.1) that together form the EU approach to CIP. The approach is guided by three strategies:

1. The CIIP dedicated strategy widely known as the European Programme for Critical Infrastructure Protection (EPCIP), which was adopted in 2004.
2. The European Security Strategy (since 2003).
3. The European Internal Security Strategy (since 2010).

The region's most important CIIP legislative effort is Directive 2008/114 to identify and designate European critical infrastructures, the CIP Directive. These and other EU-level CIP initiatives are discussed in more detail below.

The CIIP concept was first introduced to the EU's strategic security policy system in 2003. The motive was the recognition that ubiquitous integration of technology had increased European dependence on—and thus vulnerability to—interconnected infrastructure in transport, energy, and information, among other sectors. Security policy changes implied that EU member states also had to account for CIIP targets in their national policies.

The EPCIP, a CIP-dedicated strategy, was developed in 2004 by the European Commission, an executing arm of the EU, at the request of the

Box 2.2. Measures Taken at the EU Level to Facilitate Implementation of the EPCIP

A number of strategic initiatives facilitating research and development, capacity building, and connectivity among stakeholders involved in CIP were established under the EPCIP umbrella.

The Prevention, Preparedness, and Consequence Management of Terrorism and Other Security-Related Risks program was designed to protect citizens and critical infrastructures from terrorist attacks and other security incidents by fostering prevention and preparedness, namely by improving the protection of critical infrastructures and addressing crisis management. The key objective was to support CIP policy priorities by offering expert knowledge and a scientific basis to better understand the critical nature and interdependencies at all levels. Under the EPCIP, the European Commission funded over 100 projects from 2007 to 2012.

The Critical Infrastructure Warning Information Network (CIWIN) portal was established as an internet-based multi-level system to exchange CIP ideas, studies, and good practices. The portal, which has been up and running since mid-January 2013, also serves as a repository for CIP-related information. This initiative seeks to raise awareness and contribute to the protection of critical infrastructure in Europe.

The European Reference Network for Critical Infrastructure Protection was created to “foster the emergence of innovative, qualified, efficient, and competitive security solutions, through networking of European experimental capabilities.” It aims to link existing European laboratories and facilities to carry out critical infrastructure-related security experiments and test new technologies, such as detection equipment.

Source: Authors based on European Commission (2006).

European Council. The EPCIP was the first high-level EU document instituting the basic CIP pillars for the whole region. It also recognized and described the threats that could result in the loss of vital services and set the aim to enhance the EU’s CIP capability. In particular, EPCIP originated the following:

- A description of critical infrastructure.
- Selection criteria to determine whether a particular infrastructure or element of an infrastructure is critical.
- General merits of the critical infrastructure security management process.

The EPCIP applies to EU member states and three member countries of the wider European Economic Area.[1]

All the EU member states are guided by the EU-level strategy and are obliged to transpose the strategy’s pillars nationally. This principle underpins the CIP system across the EU. To facilitate this process, in 2008, the European Commission issued a Communication on the EPCIP, designing the process of implementation in member states (Table 2.1). Implementing the EPCIP was supported by a number of different initiatives, including support for national research and development efforts in CIP (Box 2.2).

Adopting the CIP Directive was an important step in forming the EU-level CIP legal framework. The current scope of the CIP Directive is limited to the energy and transport sectors. This was the first step in a methodical approach to identify, designate, and protect critical infrastructures at the EU level, the European Critical Infrastructures (ECI).[2] The CIP Directive requires all member states to identify, designate, and protect ECIs in the energy and transport sectors; it indicates the information and communications technology (ICT) sector as a priority for possible future expansion of its scope.

[1] The European Economic Area, which includes the EU countries plus Iceland, Liechtenstein, and Norway, allows the three additional countries to be part of the EU’s single market.

[2] Critical from a European perspective refers to a situation where disruption of a critical infrastructure would have an impact on at least two member states.

The Directive mandated that the responsibility to protect critical infrastructures, including national and European infrastructures, lies with the member states and with the owners/operators of critical infrastructures. It imposed fulfilling a series of obligations and undertaking certain actions. For instance, the CIP Directive requires owners/operators of designated ECIs to prepare operator security plans and advanced business continuity plans and to nominate Security Liaison Officers, thereby linking the owner/operator with the national authority responsible for CIP. The CIP Directive also defines key CIP terms such as critical infrastructure, European critical infrastructure, risk analysis, sensitive CIP-related information, protection, and owners/operators of ECIs. It specifies that member states had to take the necessary steps to comply with the Directive by January 12, 2011. The EU member states transposed the provisions of the Directive by incorporating them into their national legislative and regulatory frameworks. They used a variety of technical and legal approaches, such as amendments to existing laws and regulations, new laws, resolutions, procedural changes to existing CIP-related activities, and decrees and executive orders. Specific examples of the CIP Directive's transposition in Finland, the UK, and Spain are described in more detail below.

In 2009, CIP became an integral part of the EU-level program with the formulation of a roadmap for EU work in justice, freedom, and security for the period 2010–14 known as the Stockholm Programme. The program aims to meet challenges and strengthen justice, freedom, and security with actions focusing on the interests and needs of citizens. One of its objectives is to reduce critical infrastructure vulnerabilities. Moreover, it provided strategic guidance and basis for the Council, the Commission, the European Parliament, and the member states to draw up and implement policies to further improve measures for the protection, security preparedness, and resilience of critical infrastructure, including ICT and services infrastructure.

The EU's CIIP framework further evolved in 2010, when CIIP was referenced in the EU Internal Security Strategy as a security threat. The strategy called for better protected critical infrastructures from criminals who take advantage of modern technologies. It also recognized that the EU should continue its work in protecting critical infrastructures because they are essential for society and the economy to function. The strategy also emphasized that these threats call for improvements to long-standing crisis and disaster management practices in terms of efficiency and coherence.

Currently, the region is reviewing the CIP Directive and EPCIP. Both are the result of the Stockholm Programme, which stressed strengthening incentives to further legislative efforts. One of the motivations to review the CIP Directive was the potential need to increase the number of critical infrastructure sectors beyond transport and energy. The review was conducted in 2012 in close cooperation with the member states and relevant stakeholders.[3] In 2013, the review process resulted in a European Commission Staff Working Document that suggested a new approach for the EPCIP.[4] The document suggested more practical implementation of CIP activities under the three main pillars: prevention, preparedness, and response. Among others, new approaches aimed to take better account of interdependencies between critical infrastructures. During the drafting of this publication, the EPCIP was being amended and the review of the CIP Directive was still in progress.

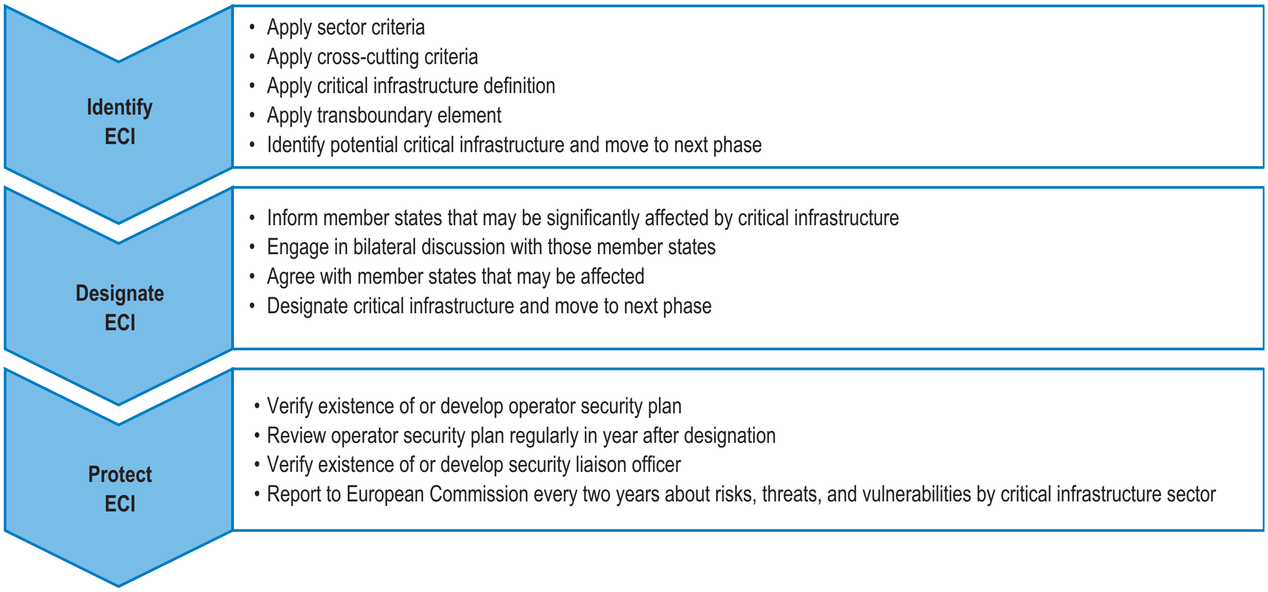
Governance and Regulation

From the standpoint of governance and practical implementation at the EU level, the ECI protection process is divided into three phases: identification, designation, and protection of ECI (Figure 2.1). Since 2013, the EU has been piloting a new, more engaged approach to EPCIP.

[3] See staff working document adopted in 2012 listed in Table 2.1.

[4] See staff working document adopted in 2013 listed in Table 2.1.

FIGURE 2.1. Phases for Governance and Regulation of European Critical Infrastructure Protection



Identify ECI

- Apply sector criteria
- Apply cross-cutting criteria
- Apply critical infrastructure definition
- Apply transboundary element
- Identify potential critical infrastructure and move to next phase

Designate ECI

- Inform member states that may be significantly affected by critical infrastructure
- Engage in bilateral discussion with those member states
- Agree with member states that may be affected
- Designate critical infrastructure and move to next phase

Protect ECI

- Verify existence of or develop operator security plan
- Review operator security plan regularly in year after designation
- Verify existence of or develop security liaison officer
- Report to European Commission every two years about risks, threats, and vulnerabilities by critical infrastructure sector

Source: Authors based on European Commission (2012).

The pilot aims to optimize the protection and resilience of four selected European critical infrastructures (EC, 2013):

- European Organization for the Safety of Air Navigation (Eurocontrol)
- Galileo, a global navigation infrastructure under civil control, consisting of 30 satellites and the associated ground infrastructure
- Electricity transmission grid
- Gas transmission network

The four critical infrastructures were selected on the basis of:

- **Cross-border** both physically (i.e., the infrastructures are located in the territory of more than one member state) and at the level of the service provided (i.e., a disruption of service in one member state could affect several other member states, causing a domino effect).
- **Cross-sector** in that they cover the transport, space, and energy sectors.
- **Interest of the operators/owners** to participate in the pilot and share their experiences.

Throughout the pilot, the European Commission analyzed how to increase the dialogue between the operators/owners of the critical infrastructures and all actors across Europe who would be affected by an event compromising the functionality of the critical infrastructures. In 2014, the Commission set a roadmap after which the Commission's report on progress and the next steps should follow. Some actions, responsibilities, and timelines are presented in Table 2.2. The table represents a governance model for ECI protection at the EU level and within the European Commission. This is an internal process formed within the European Commission and its relationship with the member states. It would be a good example of how the CIP approach could be developed and implemented in any other region, including LAC, as a whole or in separate countries.

The Directorate General for Migration and Home Affairs (DG HOME) is a structural unit of the European Commission that manages policies that aim to ensure all activities necessary and beneficial to the economic, cultural, and social

TABLE 2.2 Distribution of Roles and Responsibilities for ECI Protection at the EU level

Action 1: Design EU approach to protect and increase resilience of ECI	Actor	Timeframe
Detailed assessment and analysis of processes and methodologies used in the selected cases.	DG HOME[a] (lead), JRC[b] (support), and selected stakeholders	Starting in the second half of 2013
Agree on the criticalities and interdependencies of the selected cases. Agree on concepts, definitions, and a methodology for critical infrastructure risk assessment and risk management.	DG HOME (lead), JRC (support), and selected stakeholders	Starting in the second half of 2013
Agree on preparedness measures, such as contingency planning, stress tests, awareness raising, training programs, joint courses, and exercises and/or staff exchanges.	DG HOME (lead), JRC (support), and selected stakeholders	Starting in the second half of 2013
Explore the possibilities for establishing teams of EU recovery specialists in case of a major critical infrastructure failure to help with long-term recovery of critical services and to be deployed at the request of member states.	DG HOME and DG ECHO[c]	Starting in the second half of 2013
Assess achieved results and identified gaps.	DG HOME (lead) and JRC (support)	First half of 2014
Discuss and validate the EU approach by member states and stakeholders.	DG HOME, member states, and critical infrastructure operators	First half of 2014
Action 2: Broaden implementation of the EU approach	**Actor**	**Timeframe**
Identify and select other possible pan-European infrastructures to implement the developed approach.	DG HOME, member states, and critical infrastructure operators	Second half of 2014
Implement for the selected pan-European critical infrastructures. Continue consensus and dissemination of the selected approach to regions, with projects covering Euro-regions or involving a group of member states.	DG HOME (lead), JRC (support), critical infrastructure operators, and member states	Second half of 2014
Link the funds under the Internal Security Fund to implementing the developed EU approach.	European Commission	As of 2014

Source: EC (2013).
[a] DG HOME is Directorate General for Migration and Home Affairs.
[b] JRC is Joint Research Center, an in-house research center of the European Commission.
[c] DG ECHO is Directorate General for Humanitarian Aid and Civil Protection.

growth of the EU. It is the leading entity for the formation of the CIP plan within the European Commission.[5] The Joint Research Center (JRC), the European Commission's in-house research center, supports assessment and analysis activities (Table 2.2, Action 1).[6] Research institutions routinely and systematically participate in assessing and assigning CIP, which is the most resource consuming activity. Considered to be the best practice, this assessment and assignment enables outsourced scientific and research capacity that is usually not available in public institutions. When discussing the contingency and mitigation measures in case of major critical infrastructure disruptions, the European Commission also involves its Directorate General for Humanitarian Aid and Civil Protection (DG ECHO) to support long-term recovery of critical services.[7] For the purpose of the pilot exercises, owners/operators of critical infrastructures were also closely involved. The results of the pilot clarified the CIP approach at the regional level and were closely discussed with all EU member states. At the time of writing this publication, the activities listed in Table 2.2 were not finalized.

[5] http://ec.europa.eu/dgs/home-affairs/index_en.htm.
[6] https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection.
[7] http://ec.europa.eu/echo/.

CIIP Policy and Governance in Finland

Strategy and Legislation

Finland's CIIP policy is part of its national security framework. The main objectives of the framework are to secure functioning of the society, analyze risks, commission a governance model for emergency situations, and put in place responsibilities for all the actors, including private sector and nongovernmental organizations. One of Finland's earlier security strategies (2006) captured the notion of CIIP as the "functioning of the economy and infrastructure" pillar of the Strategy for Securing the Functions Vital to Society (Finland, 2006a). This strategy included seven vital functions (Box 2.3). During its conception, the document outlined nine threat scenarios related to disruption of critical infrastructures and 61 associated special situations.

This logic and the overall structure of the strategy were based on an updated version of the Society Security Strategy (Katri Suvando, 2011) written in 2010. Similar to the previous strategy, securing vital functions is maintained by implementing 18 strategic tasks that are associated with each vital function. The CIIP strategic tasks include acquiring and allocating funds, safeguarding insurance services, securing the fuel supply, preserving electric power, defending ICT systems, and guaranteeing housing.

The critical infrastructure sectors and protection policies are defined in the *Security of Supply Act* and in the Decree of the National Emergency Supply Agency. Line ministries are responsible for securing vital functions within their respective competencies. This approach facilitates formulating and subsequently implementing CIIP-related provisions throughout the different sectors.

Protection of each critical infrastructure is defined and implemented through separate sectoral strategic documents. For instance, general provisions for CIIP are established in a horizontally applied strategic document dedicated to the growth of Finland's information society, the National Knowledge Society Strategy 2007–15 (Finland, 2006b). The document emphasizes the importance of the security of information networks so citizens can trust electronic services. In addition, it highlights the importance of well-functioning substructures, stating that information networks depend on basic infrastructure, such as electricity supply, and emphasizing that security of supply of services for the information society is especially important in crisis situations. Further, the CIIP notion is elaborated in the Cyber Security Strategy (Finland, 2013) that was adopted in 2013. In this strategy, Finland recognizes that "national law should be considered from the perspective of international and EU legislation." When dealing with cross-border and increasingly regional and global threats, discrepancies in national legislation may not be sufficient to protect national interests. The document also enacts a number of principles that are fundamental for CIIP and considers the role of CII in other critical infrastructures.

In particular, within the ICT sector, but also in other sectors, most of the critical infrastructures in Finland are privately owned and/or operated.[8] Public sector companies, for the most part, provide cyber know-how and expertise, as well as security services and defenses. For this reason, a national approach to CIIP policy and legislation needs to meet the existing environment and focus on raising CIIP competencies within business activities. This system also seeks to build awareness and strengthen cooperation between private sector and relevant CIIP authorities.

Governance

The Government of Finland exemplified strong political leadership and responsibility for providing strategic guidelines and making the required decisions regarding allocating resources and prerequisites for CIIP. The Security Committee, which is authorized under the Security Strategy for the

[8] The UK is similar, with 80 percent of critical infrastructure assets owned by the private sector. In the United States, 85 to 90 percent of critical infrastructure is privately owned.

Box 2.3. CIIP as Part of Finland's Strategy for Securing the Functions Vital to Society

The Strategy for Securing the Functions Vital to Society was adopted in 2006 and aimed "to safeguard the country's independence, preserve security in society, and maintain the livelihood of the population." It also sets out the government's guidelines for its line ministries.

The following functions were defined as vital:

1. Management of government affairs
2. International activity
3. National military defense
4. Internal security
5. Functioning of the economy and infrastructure
6. The population's income security and capability to function
7. Psychological crisis tolerance

One of the seven vital pillars—functioning of the economy and infrastructure—is defined as follows:

"The functioning of the economy refers to the economic exchange which meets the population's and the business community's basic needs and supports a sufficiently healthy state economy. The maintenance of infrastructure means the technical structures and organizations, which are necessary to provide a livelihood for the population and for the functioning of society. This entirety includes the safeguarding of the state economy, the financial market and the insurance business as well as securing the electronic ICT systems and transports. Furthermore, sustaining society's basic economic functions, a competent labor force, preserving a first-rate education system and research structure as well as understanding and adapting to the changes in the environment are also included."

This definition encompassed the understanding that the state should maintain the sustainable and safe operation of the economy as a whole from fiscal, taxation, and other standpoints, but also references the protection of critical infrastructures such as energy, finance, ICT, and transport.

The 2006 strategy was amended in 2010, but the logical flow was maintained. For instance, the vital functions for society remained the same.

Source: Authors based on Finland (2006a).

Society, monitors and coordinates the implementation of activities.

Security and disturbance management require the government and different actors to have reliable, real-time monitoring of the condition of society's vital systems, including disturbances that affect their functioning. Each ministry and administrative branch is responsible for CIIP and disturbance management within its mandate and must carry out strategic tasks determined on the basis of the desired end states. The CIIP regulatory system is based on the clear assignment of relevant tasks, service agreements, and common security management standards of the respective authorities and actors in the business community. Each administrative branch assesses risk and analyzes security maturity to find any significant cyber security vulnerabilities and risks and the level of their readiness to respond to cyber-attacks.

In Finland, there are two major public agencies dealing with CIIP. The National Emergency Supply Agency (NESA)[9] is a CIP-dedicated agency and cross-sector administrative operative authority for the security of supply of critical services in Finland. NESA is part of the Ministry of Employment and

[9] See http://www.nesa.fi/security-of-supply/.

the Economy and is responsible for economic preparedness, coordinating preparations within the public administration, and developing and maintaining the security of the supply chain. The National Emergency Supply Council (NESC) is the body that gathers experts from the private sector and focuses on analyzing threats. Together NESA and NESC formulate plans and guidelines for public authorities and businesses with respect to managing and controlling threats and risks. NESA also has a role in securing critical infrastructures by developing and financing technical backup systems and electromagnetic pulse to secure premises for electronic systems. It has also participated in preparing EPCIP and CIWIN.

In addition to the above cross-sectoral bodies, for critical infrastructures there are sectoral agencies. For CIIP, the central government's data security and information management policies are steered and developed by the Ministry of Finance. The Government Information Security Management Board, acting under the Ministry of Finance, processes and coordinates the central government's key information security and cyber security guidelines.

Another CIIP body is the Finnish Communications Regulatory Authority[10] (FICORA) within the Ministry of Transport and Communications. FICORA is a general regulatory authority for issues concerning electronic communications and information society services. FICORA's mission includes issuing technical regulations and coordinating standardization at the national level. It also oversees the protection of privacy and securing data in electronic communications. FICORA also ensures that telecommunications operators are prepared for emergencies. The operators must report to FICORA any significant information security incidents as well as any threats, faults, or disturbances in telecommunication networks and services. Generally speaking, FICORA is the agency responsible for the security of electronic communications networks that link critical infrastructure sectors. For other critical infrastructures, such as transport or energy, sectoral agencies will be different.

CIIP Policy and Governance in the UK

Strategy and Legislation

The impulse to enhance the UK's CIIP framework was the devastating floods the country faced in 2007, which was considered the country's largest emergency situation since World War II. The floods cost the UK economy over £4 billion and the damage, specifically to critical infrastructure, was valued at about £674 million. Crisis management activities undertaken at the time proved that things could have been handled more efficiently and have been better organized and coordinated. *The Pitt Review: Lessons Learned from the 2007 Floods* (Pitt, 2008) was commissioned to undertake a comprehensive review of the processes implemented during the event and recommendations to strengthen the national CIIP framework against natural hazards. Specifically, the review called for a more systematic approach to building resilience in critical infrastructure. It suggested a cross-sector campaign involving owners/operators, regulators, and government to improve the resilience of critical infrastructure and essential services (today known as the Tripartite approach, as shown in Box 2.4) especially to disruptions from natural hazards. In many respects, further evolution of the UK's CIIP framework is a follow-up to the emergency events of 2007.

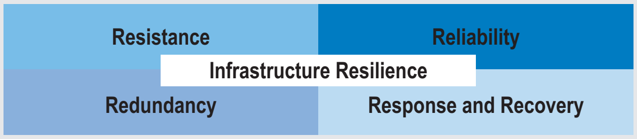
The National Security Strategy guides the overall approach for the UK's CIIP. The country's national security framework (similar to Finland's) encompasses the notion that a strong economy is a vital basis for national security. Thus, the strategy aims to ensure a secure and resilient environment within the UK in the context of the selected risks. To these ends, the UK government implemented its annual National Risk Assessment (NRA) in 2008. An NRA is intended to capture the range of emergencies that might have a major impact on all or significant parts of the nation. It focuses on domestic civil emergencies that are most likely to materialize

[10] https://www.viestintavirasto.fi/en/index.html.

Box 2.4. The UK's Approach to Building Infrastructure Resilience

In the UK, infrastructure resilience is defined as the ability of assets and networks to anticipate, absorb, adapt to, and recover from disruption. Resilience is secured through a combination of the principal components shown in Figure 2.2.

FIGURE 2.2. Phases for Governance and Regulation of European Critical Infrastructure Protection



Source: Authors based on European Commission (2012).

Resistance concerns direct physical protection (e.g., erecting flood defenses). **Reliability** is the ability of infrastructure to maintain operations under a range of conditions (e.g., electrical cabling can operate in extremes of heat and cold). **Redundancy** is the adaptability of an asset or network (e.g., the installation of back-up data centers). **Response and Recovery** is an organization's ability to respond to and recover from disruption.

Tripartite Approach: The appropriateness and cost-effectiveness of each component varies across the sectors because of, for example, the different types of infrastructure, technical opportunities, and business models. Infrastructure owners should work with government and regulators to select the blend of these components that will produce the most cost-effective and appropriate strategy.

Source: Authors based on UK (2010a).

within the coming five years. While an NRA is a confidential evaluation, the government publishes the document, which is known as the National Risks Register (NRR). The objective of the NRR is to advise people and businesses on how they can better prepare for civil emergencies.[11] The NRR also provides useful information regarding how the UK and its emergency services prepare for these risks.

The UK's most recent National Security Strategy, published in 2010 (HM Government, 2010), introduced innovations. For instance, a new exercise, a National Security Risk Assessment (NSRA) was put into practice.[12] This exercise aims to assess and prioritize all major areas of security risks nationally, domestically, and overseas. Different from an NRA, an NSRA goes beyond domestic risks and is repeated every two years.

In 2010, the government adopted the "Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards" (UK, 2010a). The document expands on principles (Box 2.4) and cross-sector programs. It lays down the roles and responsibilities of public bodies. In 2011, the strategic framework was complimented by the "Guide to Improving the Resilience of Critical Infrastructure and Essential Services" (UK, 2011). The guide includes principles of infrastructure resilience, the foundation of building processes, and guidance on various practices (e.g., hazards, checklists, and information sharing).

Starting in 2009, at the sector level, the UK government launched preparations for the annual sector resilience plans for each of the nine critical infrastructure sectors that had been identified. The sectoral approach is important as owners and operators of critical infrastructures do not all face the same set of risks and neither do they tackle the security issues in the same manner. The differences

[11] See National Risk Register, 2012 edition, at: https://www.gov.uk/government/publications/national-risk-register-for-civil-emergencies-2012-update.

[12] Risk assessement and prioritization methodology is described in the appendix of the National Security Strategy.

Box 2.5. **Summary of UK Sector Resilience Plans**

Sector resilience plans set out the resilience of each critical national infrastructure (CNI) sector in relation to the relevant risks identified in the NRA. The sector resilience plans provide guidance to sector actors related to protecting CNI, including nuclear and hazardous sites, and offer priority actions to increase the level of resilience.

For instance, the 2013 Sector Resilience Plan called actors to ensure that resilience plans incorporate the risk of cyber-attacks. In the energy sector, one of the priorities identified was a need to perform risk assessments for oil and gas beach terminals from fluvial and coastal flooding. For the finance sector, the major risks identified were disruption to energy and communications networks and damage to or destruction of key financial assets and networks.

Source: Authors based on Guthrie and Konaris (2012); UK (2013a).

across critical infrastructure sectors and geographical locations mean there is no one size fits all approach to improving resilience. Sectoral plans are prepared in close cooperation with relevant regulatory agencies and private sector actors (Box 2.4). Sector resilience plans are written in relation to the risks identified in current NRAs. Although individual plans are confidential, the unclassified summary of sector resilience plans is released annually.[13] The summary provides overall information about the resilience of each critical infrastructure sector separately, identifies the risks and vulnerabilities, the desirable level of resilience, a program of actions for achieving the desired level, and methods of reporting on progress toward achieving it (Box 2.5).

When it comes to specific critical infrastructure segments, referred to as critical national infrastructures (CNI), there are dedicated sectoral policies and regulations. Strengthening the sectoral CIIP approach is, among other functions, performed through the independent reviews requested by the government for the particular sector.[14] Afterward, the government reports on implementing the relevant recommendations and further activities to improve the resilience of the CNI.[15]

Examining the sectoral policies for CIIP, the UK has adopted two major strategic frameworks: the National Information Assurance Strategy (UK, 2007) and the Cyber Security Strategy (Cabinet UK, 2015). The first aims to provide ongoing assurance to the government that the risks to information systems and the information they hold are appropriately managed. One of the main government targets for 2015 was to achieve reduced vulnerabilities in government systems and critical infrastructures. The second document is dedicated to securing the UK's cyber space. It is implemented through the National Cyber Security Programme, which allocates financial resources and activities dedicated to CIIP (Box 2.6).

Governance

In the UK, the main responsibility for resilience of critical infrastructures lies with the owners and operators of the infrastructure. The government,

[13] The annual summary of Sector Resilience Plans for 2010–14 can be found at: https://www.gov.uk/government/collections/sector-resilience-plans.

[14] Performed by the independent parties.

[15] For instance the resilience review for the transport sector was published in 2014, followed by the government's response to the review in 2015. Both documents can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/417406/transport-resilience-review.pdf; https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/380213/cm-8968-accessible.pdf.

A review of the energy sector was undertaken by the House of Lords Science and Technology Committee and the government's report was published in June 2015. The response of the government can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/440286/50226_Cm9083_Gov_response_to_HoL_report_Accessible.pdf.

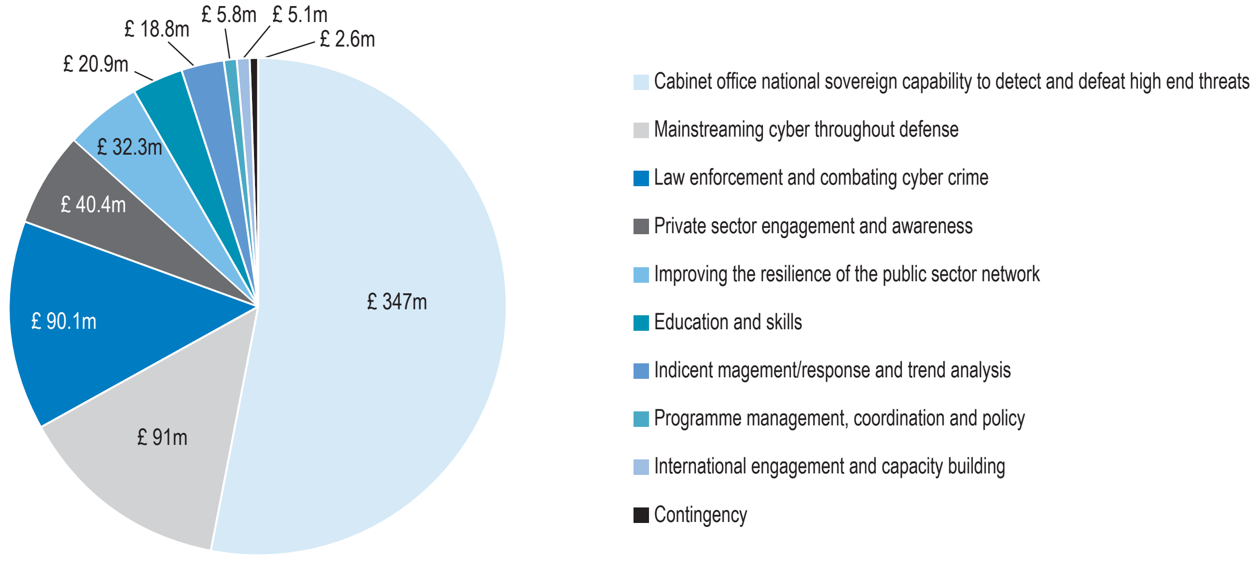
Box 2.6. What It Costs to Implement the UK's Cyber Security Strategy

To achieve the objectives of its National Cyber Security Strategy, the UK has set aside £650 million (US$960 million) of public funding for a four-year National Cyber Security Programme. The total budget dedicated to implementing the strategy is £860 million (until March 2016).

During the first three years of implementation, nearly two-thirds of the 2011–13 budget (£253.8 million) was spent on technical capabilities to detect and respond to the most sophisticated threats. Most of these activities were dedicated to increasing the resilience of critical infrastructures against cyber threats. During the fourth year (2013–14), the budget allocated for this purpose was slightly less than half (£93.2 million). The second and third largest expenditure lines were dedicated to cyber defense and combating cyber-crime.

Another of the strategy's big priorities (and also expenditures) was engaging with the private and public sectors. For that purpose, the UK, through the Home Office, the Department for Business, Innovation & Skills and other delivery partners, spent £19.3 million in 2011–14 and planned to spend £21.1 million in 2014–15. The National Cyber Security Programme's objectives were to improve awareness of the cyber threat among businesses and the public, reduce the number of attacks on businesses, ensure a coherent approach across the government, and work with those responsible for CNI to improve its protection.

FIGURE 2.3. Total Planned Expenditures per Activity of the National Cyber Security Programme, 2011–15 (in British pounds)



Source: Nao (2014).

regulators, and industry work closely together to ensure future infrastructure investments consider the needs for security and resilience. The requirements for investments in critical infrastructure related to improving security and resilience are guided by the following three principles:

- Investments should be proportionate to risks.
- Investments should be enabled by improved sharing of information between those who need to know.
- Investments should be delivered at the lowest practicable level.

TABLE 2.3. Departments Leading Responsibility for Critical Infrastructures in the UK

Sector or subsector	Government departments
Communications	Department for Business, Innovation, and Skills
Ambulance*	Department of Health
Fire*	Department for Communities and Local Government
Coastguard*	Department for Transport
Police*	Home Office
Energy	Department for Energy and Climate Change
Finance	HM Treasury
Food	Department for the Environment, Food and Rural Affairs, and Food Standards Agency
Government	Cabinet Office
Health	Department of Health
Transport	Department for Transport
Water	Department for the Environment, Food and Rural Affairs

Source: Authors.
*These subsectors belong to the emergency services critical infrastructure sector but are presented separately because the governance bodies are different.

At the national level, the Cabinet Office and the Centre coordinate the CIIP framework for the Protection of National Infrastructure (CPNI).[16] The Cabinet Office is the supreme governmental body that decides on CIIP-related issues of major importance. For instance, this office aggregates sectoral resilience plans for critical infrastructure.[17] Produced annually, the plans are provided to ministers to alert them of any perceived vulnerabilities, with a program of measures to improve resilience where necessary. The Cabinet Office also decides on the allocation of national funds to implement CIIP.

In addition, the CPNI provides security advice and liaises with the Civil Contingencies Secretariat of the Cabinet Office, which works to enhance the nation's ability to prepare for, respond to, and recover from emergencies. It works closely with the police and has a strong partnership with the National Counter Terrorism Security Office and the nationwide network of police specialists, the Counter Terrorism Security Advisers. The Cabinet Office and these security advisers also support CPNI in providing guidance on securing critical sites within the critical infrastructures.[18]

At the sector level, relevant government departments take the lead in ensuring appropriate steps are taken within their jurisdiction to improve protective security (Table 2.3). They also identify critical infrastructures within their areas in consultation with CPNI and relevant organizations.

CIIP Policy and Governance in Spain

Strategy and Legislation

The major advancements in CIIP framework development in Spain were made in 2007 with the approval of the very first National Plan for Critical Infrastructure Protection and National Catalogue of Strategic Infrastructure. Also in 2007, the government approved an agreement on Critical Infrastructure Protection authorizing the governance framework to direct and coordinate the necessary actions to protect critical infrastructures (Spain, 2007). This paved the way for the establishment of the National Centre for Critical Infrastructure Protection (CNPIC) under the Ministry of the Interior.

[16] http://www.cpni.gov.uk/.
[17] https://www.gov.uk/government/collections/sector-resilience-plans.
[18] See more at: http://www.cpni.gov.uk/about/Who-we-work-with/#sthash.vM6V5SwC.dpuf.

Box 2.7. Regulation of Protection of Critical Infrastructure in Spain

After adopting Law 8/2011 regarding protecting critical infrastructure, the Ministry of the Interior issued regulations providing detailed guidance on the following issues:

National Catalogue of Critical Infrastructures: Includes list of critical infrastructures. Provides objectives and describes the information update procedures and governance framework for the Catalogue.

Governance Model for CIP: Defines roles and functions of the institutions involved in CIP, including private critical infrastructure operators.

The regulations specify the following for **the CIP plans that are maintained in Spain** (i.e., the national CIP plan, sectoral CIP plans, the security and operational plans of critical infrastructure operators, and operational support plans):

- For each type, development objectives and process.
- For sectoral plans and plans for critical infrastructure operators, composition and development requirements.
- For all plans, process of approval and classification.
- A review process.

Communication between critical infrastructure operators and public institutions: Defines security of communications, establishes the process of designating the critical infrastructure contact officers within the critical infrastructure operator, and provides protection for classified information.

Source: Authors based on Spain (2011).

The National Plan for Critical Infrastructure Protection sets the criteria, guidelines, and operational capabilities to ensure protection of critical infrastructures from various threats, both generic and specific. The National Catalogue of Strategic Infrastructures contains a complete, updated, and verified list of all crucial domestic infrastructures. It consists of specific characteristics of each critical infrastructure, such as its location, ownership, scope of service provided, safety, and criticality level. Both documents are constantly updated and are classified in accordance with national legislation.

In 2011, Spain adopted legislation (Jefatura del Estado, 2011) that set the overall governance framework for CIIP, designating 12 critical infrastructure sectors and various protection measures (Box 2.7) (Spain, 2011). Those legal acts formed the basis of the national CIIP legal framework.

Apart from maintaining the national CIIP plan, the law mandated preparation of strategic sectoral plans to define protection activities in each of the critical infrastructure sectors identified in the CIIP framework. Moreover, it created procedures to designate the critical infrastructure operators. In this regard, critical infrastructure operators are tasked with a set of functions and obligations related to maintaining certain security levels. The regulation of CIIP processes is further elaborated in Box 2.7. In June 2014, the government adopted plans for five critical infrastructure sectors (electricity, gas, oil, nuclear, and financial) and designated 37 new operators of critical infrastructure. In January 2015, a commission was organized to review the work done to prepare the sectoral plans for the critical infrastructures in the transport and water sectors.[19]

[19] http://www.interior.gob.es/es/web/interior/noticias/detalle/-/journal_content/56_INSTANCE_1YSSI3xiWuPH/10180/3188420/?redirect=http://www.interior.gob.es/es/web/interior/prensa/noticias?p_p_id=101_INSTANCE_GHU8Ap6ztgsg&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1l

Additionally, Spain is one of the countries where the national government empowers provincial and regional authorities, thus Spain had to take additional legislative steps to coordinate the CIIP framework and delegate certain activities to the regions and cities that are granted autonomy. Provincial and regional authorities participate in the CIIP processes under the coordination of the government through the Secretary of State for Security.

On the policy side, protection of critical infrastructure falls under the strategic framework of national security within the first National Security Strategy, which was adopted in June 2011.[20] Critical infrastructures, services, and supplies were explicitly included among nine other threat and risk areas identified. The strategy provided high-level guidance for CIIP and formed the groundwork for further legislative initiatives and governance. In 2013, the current National Security Strategy (Spain, 2013a) was adopted. It included seven lines of action:

1. Shared responsibility and public–private cooperation
2. Tiered planning
3. Balance and efficiency
4. Resilience
5. Coordination
6. International cooperation
7. Safeguarding the security of critical infrastructure in accordance with the National Plan of Critical Infrastructure

Further, the National Cyber Security Strategy guides the CIIP framework. It aims to be aligned with initiatives similar with those of the region and with relevant international organizations, particularly the EU Cyber Security Strategy. The National Security Strategy mandated preparation of the first Cyber Security Strategy in 2011 and the current National Cyber Security Strategy (Spain, 2013b) was adopted in 2013.

Governance

The Prime Minister directs and supervises implementation of the National Security Strategy through the framework of the National Security Council. Its approach includes lines of actions related to CIIP and implementing the National Cyber Security Policy.

The CIP Law mentioned in the previous section authorizes the governance framework for CIIP. On the policy level, the Secretary of State for Security under the Ministry of the Interior coordinates efforts. Main actors and their key functions are listed in Table 2.4. The CNPIC[21] coordinates and works closely within 12 critical infrastructure sectors to define specific security priorities and maintains the National Catalogue of Critical Infrastructures. CNPIC is a point of reference for both CIP and CIIP (Theodore Puskas Foundation, 2013) nationally and internationally.

Dedicated committees perform other important functions. Two examples are the National Committee for Critical Infrastructure Protection and the Interdepartmental Working Group on Critical Infrastructure Protection. The former approves sectoral strategic plans and designates the critical infrastructure operators. The latter develops those plans and suggests operators that could be nominated as critical infrastructure operators. Both organizations include representatives from autonomous regions and cities and are led and coordinated by CNPIC.

Moreover, line ministries and public institutions assigned for each critical infrastructure sector are leading sectoral CIIP efforts. Assignment of the ministries and public institutions is performed through the CIP Law (Table 2.4).

CIP and CIIP Policy and Governance in Korea

Different laws in Korea address CIP and CIIP. The country began its digitalization campaign in the 1980s and, as a result, understood the need to protect digital records, privacy online, and the

[20] SpanishSecurityStrategy:Everyone'sresponsibility,2011:at: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lang=en&id=130671.

[21] http://www.cnpic.es/index.html.

TABLE 2.4. Main Actors of CIIP Governance in Spain

No.	Institution	Main functions
1.	Secretary of State for Security within the Ministry of the Interior	Coordinates national CIIP efforts and heads the governance framework. Chairs the commission for critical infrastructure protection.
2.	National Center for Critical Infrastructure Protection (CNPIC) established under the Ministry of the Interior	Manages classifying and updating the National Catalogue of Critical Infrastructures. CNPIC is responsible for coordinating and supervising the protection of national critical infrastructures and is designated as the Spanish National Point of Contact at the international level.
3.	Ministries assigned for each critical infrastructure sector	Promote and implement the CIIP security policies within their respective competencies and critical infrastructure sectors.
4.	Autonomous communities and cities with a statute of autonomy	Participate in CIIP process within their territories (e.g., declaring an area within its territory as critical and approving operational support plans). Participate in the National Commission on Critical Infrastructure Protection and meet with the interdepartmental working group.
5.	National Commission for the Protection of Critical Infrastructure	Approve Sectoral Strategic Plans and designate critical infrastructure operators that are proposed by the interdepartmental working group for CIIP. The Commission is a collegial body chaired by the Secretary of State for Security.
6.	Interdepartmental Working Group for Critical Infrastructure Protection	Develop Sectoral Strategic Plans and propose nominations for critical infrastructure operators.
7.	Public and private operators of critical infrastructure	Cooperate with the authorities that comprise the national CIIP system. Provide technical advice on composing the catalogue of critical infrastructure. Provide updated information about critical infrastructure. Participate in preparing sectoral strategic plans and in risk assessment exercises. Prepare operational security plans. Appoint safety liaison and contact point in case of European critical infrastructure.

Source: Authors based on Jefatura del Estado (2011); further actors and functions are established by the regulation on CIP approved by the Royal Decree 704/2011, May 2011.

criticality of information infrastructure earlier than other countries. This led to early actions for CIIP. For that reason, this study looks at Korean CIP and CIIP frameworks separately. The latest of the policies remains one of the oldest frameworks globally.

Legislation and Governance: CIP

In 2004, Korea adopted the *Act on the Management of Disasters and Safety* (hereinafter referred to as ROK CIP Law), which installed a disaster and safety control system against various disasters to ensure citizen security, physical safety, and safety of property (ROK , 2010). Within the ROK CIP Law, incidents include natural disasters, accidents beyond a certain scale, and debilitation of the national backbone systems for energy, communications, and transportation, among others (Choi, Yoon, and Shin, 2014). The Enforcement Decree elaborates on implementing the ROK CIP Law ROK, 2015).

The governance model involves various stakeholders, as shown in Box 2.8. The ROK CIP Law mandated preparation of CIP plans that aim to define the activities in each of the critical infrastructure sectors, with the plans to be evaluated annually by the Minister of Public Safety and Security. The plans are classified into four categories:

1. Protection goal and risk analysis
2. Protection source management
3. Protection activity implementation
4. Situation management

Strategy and Legislation: CIIP

The country's digitalization initiatives forced government to prioritize creating policies and enabling a legal environment to support its efforts. For instance, there was an urgent need to significantly amend the laws related to information protection. Consequently, the very first ROK CIIP Law was adopted in January 2001. This law serves as the essential legislation for various cyber incidents and consists of many articles

Box 2.8. Main Actors of CIP Governance in Korea

The **Central Safety Control Committee (Central Committee)** coordinates important policies on safety control and consults and coordinates between the related ministries. The Central Committee is chaired by the Prime Minister.

The **Prime Minister** prepares and confirms development guidelines for basic plans for national safety control duties and instructs the heads of relevant central administrative agencies.

A **coordination committee** is established under the Central Committee to consult on and coordinate minor matters.

Local committees deliberate safety control plans in the relevant areas, and consult and coordinate the safety control affairs performed by the disaster control agency.

The **heads of relevant central administrative agencies** designate national infrastructures deemed necessary to be continuously managed to protect the national backbone systems after undergoing deliberation thereon by the Central Committee. They also prepare basic plans for safety control duties to be submitted to the Prime Minister.

Source: Authors based on ROK (2010).

defining CII, outlining protective measures and counters against cyber incidents, defining the work of information security consulting agencies, and specifying legal responsibilities and penalties for various entities. It also outlines the governance framework for CIIP and defines the roles and functions of the Committee for the Protection of Information Infrastructure (CPII). This committee allocates tasks of relevant ministries, institutes, the technical-level committee for Incident Response, and other central administrative organizations. Other matters addressed within the ROK CIIP Law are protection, prevention, countermeasures, technical support, technological advancement, international cooperation, and penalties for cyber-crimes. The structure of the ROK CIIP Law is outlined in Table 2.5 and its main provisions are elaborated in the Box 2.9.

The Korean government and organizations are under constant cyber-attacks. Consequently, within their National Cyber Security Master Plan,[22] the government escalated cyberspace as another operational domain like the nation's territories on land, air, and sea that need a state-level defense system. Under the plan, the critical systems must be encrypted, disaster recovery systems expanded, and important data secured.

In March 2013, a sizable cyber-attack targeted major broadcasting and financial companies. This event triggered the preparation and adoption of a comprehensive national cyber security strategy by the government, the National Comprehensive Plan for Cyber Security.[23] This plan was built around four pillars (Prompt, Cooperative, Robust, Creative):

1. Enhance **prompt** response systems against cyber threats.
2. Build smart **cooperative** systems between the relevant authorities.
3. Improve the **robustness** of the protection of cyberspace.
4. Apply **creativity** to deal with cyber security.

Governance: CIIP

The CPII deliberates the designation of CIIs, policies, and protection plans and coordinates countermeasures. The CPII is chaired by the Prime

[22] National Cyber Security Master Plan, at: http://www.kcc.go.kr/user.do?mode=view&page=A05030000&boardId=1113&boardSeq=31663.

[23] National Comprehensive Plan for Cyber Security, at: http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1212488.

TABLE 2.5. Structure of the ROK CIIP Law

Chapters	Contents	
Chapter I General Provisions	**Article 1**	(Purpose)
	Article 2	(Definitions)
Chapter II System for Protecting Critical Information and Communications Infrastructure	**Article 3**	(Committee for Protection of Information and Communications Infrastructure)
	Article 4	(Functions of Committee)
	Article 5	(Establishment of Measures to Protect Critical Information and Communications Infrastructure)
	Article 5–2	(Ascertaining Implementation of Measures to Protect the Critical Information and Communications Infrastructure)
	Article 6	(Establishment of Plans for Protecting Critical Information and Communications Infrastructure)
	Article 7	(Support for Protecting of Critical Information and Communications Infrastructure)
Chapter III Designation and Analysis of Vulnerabilities of Critical Information and Communications Infrastructure	**Article 8**	(Designation of Critical Information and Communications Infrastructure)
	Article 8–2	(Recommendation for Designation of Critical Information and Communications Infrastructure)
	Article 9	(Analysis and Evaluation of Vulnerabilities)
Chapter IV Protection of Critical Information and Communications Infrastructure and Response to Intrusion Incidents	**Article 10**	(Protection Guidelines)
	Article 11	(Orders for Protection Measures)
	Article 12	(Prohibition Against the Intrusion of Critical Information and Communications Infrastructure)
	Article 13	(Notification of Intrusion Incidents)
	Article 14	(Restoration Measures)
	Article 15	(Organization of Headquarters for Countermeasures)
	Article 16	(Information Sharing and Analysis Center)
Chapter V	Removed on May 22, 2009	
Chapter VI Technological Support and Private Cooperation	**Article 24**	(Technological Development)
	Article 25	(Support for the Management Organization)
	Article 26	(International Cooperation)
	Article 27	(Duty of Confidentiality)
Chapter VII Penalty Provisions	**Article 28**	(Penalty Provisions)
	Article 29	(Penalty Provisions)
	Article 30	(Administrative Fines)

Source: Act on the Protection of Information and Communications Infrastructure (ROK, 2013).

Minister and comprises vice minister-level officials of related central administrative agencies.

The primary responsibility of CII management agencies is CII protection. These agencies assess and evaluate vulnerabilities to prevent and deal with cyber incidents and institute countermeasures for CIIs in their charge. They are also responsible for notifying the relevant central administrative agencies and investigation agencies regarding the details of any incident, and rehabilitating the affected infrastructures.

As a working-level committee, the Ministry of Science, ICT, and Future Planning (MSIP) and the National Intelligence Service (NIS) form guidelines for designing relevant plans. Also, one of their major roles is to check whether protective measures are effective for the designated CII. The NIS Director and Minister for MSIP inform the head of the relevant central administrative agency of the confirmation results regarding protective measure implementation. They may ask the Korea Internet & Security Agency (KISA) to perform the confirmation on their behalf should they deem it appropriate.

Supporting agencies include KISA, information sharing and analysis centers, consulting companies specializing in knowledge information security, and the Electronics and Telecommunications Research Institute. These agencies helped install the relevant protective measures and technological support to prevent and respond to incidents.

Box 2.9. Key Provisions of the ROK CIIP Law

Initially adopted in 2001, the ROK CIIP Law represents one of the very first legal acts of this kind ever adopted globally. The law authorized key CIIP institutions and put in place grounding provisions that even today (after nearly 15 years) serve as a basis for CIIP frameworks. The following paragraphs outline the key reforms brought by the CIIP Law.

Establish the Committee for the Protection of Information Infrastructure (CPII): Subordinate to the Prime Minister's Office (Article 3).

Set obligations related to risk analysis, risk-based protection measures, and protection plans: The head of the infrastructure management organization should perform vulnerability analysis and evaluation on the facility under its jurisdiction, and form and implement protection measures for the facility. The head of the central administrative organization should create and implement the protection plan for CII by area of jurisdiction (Articles 5 and 6).

Provide technical support to CII owners and operators: Technical support for CII can be requested through the head of the national institute or specialist institute according to Presidential decree (Article 7).

Identify and designate CII: The head of the central administrative organization should designate the infrastructure recognized as one that needs to be protected from electronic intrusions as CII after deliberation by CPII (Article 8).

Notify about incidents: On discovery, the head of CII management should notify the related organization of the disruption, paralysis, or destruction of the facility under its jurisdiction due to a cyber-incident. The head of the organization should also take measures for recovery following damage and prevent the spread of damage (Articles 13, 14).

Information sharing and analysis center: Any person who intends to provide information concerning vulnerabilities, intrusion factors, and countermeasures or operate the real-time alarm and analysis system may establish and operate an information sharing and analysis center (Article 16).

Penal provisions: Those who disrupt, paralyze, or destroy CII with electronic infringement behavior such as hacking or computer virus can be imprisoned for a maximum of 10 years and fined 100 million won (equivalent to $100,000) (Article 28).

Source: Authors based on Act on the Protection of Information and Communications Infrastructure (ROK, 2013).

CIIP Policy and Governance in the United States

Strategy and Legislation

Strengthening the security and resilience of critical infrastructures against both physical and cyber threats is one of the core policy objectives of the United States. At the strategic level, protecting critical infrastructures and key assets is among the core mission areas within the President's National Strategy for Homeland Security (DHS, 2007). That priority was further elaborated at the strategic level within the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (DHS, 2003a). The strategy identifies a clear set of national goals and outlines the guiding principles that underpin the efforts of the United States to secure critical infrastructure and assets. The strategy for physical CIIP compliments the National Strategy to Secure Cyberspace (DHS, 2003b), which focuses on assigning, assessing, and protecting interconnected information systems and networks. The physical and cyber strategies

Box 2.10. Presidential Policy Directive on CIP No. PPD-21

Adopted in February 2013, the Presidential Policy Directive on CIP No. PPD-21 laid down the groundwork for the CIP framework in the United States. It supersedes the Homeland Security Presidential Directive No. HSPD-7 on Critical Infrastructure Identification, Prioritization, and Protection issued in 2003. The need for a new directive arose as a result of the shift and advance of the national CIP efforts that required clarification of the functions and responsibilities of the federal and relevant public agencies.

Directive PPD-21 guides national CIP efforts:

1. Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time.
2. Understand the cascading consequences of infrastructure failures.
3. Evaluate and enrich public–private partnerships.
4. Update the National Infrastructure Protection Plan.
5. Develop a comprehensive research and development plan.

The directive elaborates on the U.S. policy approach for CIP; defines CIP roles and responsibilities under the strategic guidance of the Secretary of the Homeland Security; puts in place three strategic imperatives that are aimed to be ensured by CIP efforts; guides CIP innovation, research, and development; provides directions on implementing the directive; and designates critical infrastructure sectors and sector-specific agencies.

Under the directive, the federal government is responsible for strengthening the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and for organizing itself to establish partnerships effectively and add value to the security and resilience efforts of critical infrastructure owners and operators.

Source: Authors based on DHS (2013a); U.S. White House (2013).

share common underlying policy objectives and principles. Together, they form the roadmap for priority areas of homeland security.

At the federal level, legal acts empowering strategic CIIP efforts are the Executive Orders of the President (also called Presidential directives), the first of which was issued in 1998 (U.S. White House, 1998). The Directive recognized certain parts of the national infrastructure as critical for both the national economy and security, coordinated the primary steps for its safekeeping, and laid the groundwork for a public–private partnership framework. The Directive, updated in 2003, elaborated on provisions to identify, prioritize, and protect critical infrastructure (U.S. White House, 2003). Since 2013, Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and the Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21) have governed the CIIP framework of the United States (Box 2.10) (U.S. White House, 2013).

In 2002, the United States also adopted legislation reorganizing and centralizing security functions at the federal level and aiming to meet existing threats and challenges, the Homeland Security Act (HSA).[24] This act leads the coordination and protection of critical infrastructure. HSA also facilitated the Critical Infrastructure Information Act 2002 (CII Act),[25] which regulates information exchange between critical infrastructure operators and public sector agencies. The objective of the CII

[24] Homeland Security Act of 2002, as amended, http://www.dhs.gov/homeland-security-act-2002.

[25] Critical Infrastructure Information (CII) Act of 2002, at: http://www.dhs.gov/publication/cii-act-2002.

Box 2.11. **The National Infrastructure Protection Plan of 2013: New Developments**

While the 2013 NIPP retains the basic building blocks of previous plans, it represents a significant evolution in several areas. For example, the updated plan:

1. Elevates security and resilience as the primary aim of critical infrastructure planning efforts.
2. Calls for the establishment of national priorities—determined jointly by public and private sector partners—that will drive action at the national level and inform the progression of goals and priorities at the sector, state, local, tribal, territorial (SLTT), and regional levels.
3. Focuses on creating a process to set critical infrastructure national priorities determined jointly by the public and private sector.
4. Directs joint decision-making by public and private sector partners initiated at the sector, SLTT, and regional levels.
5. Drives action at the federal level that in turn informs advancement of national goals and priorities.
6. Supports execution of the National Plan and achievement of the National Preparedness Goal at both the national and community levels, focusing on leveraging regional collaborative efforts.
7. Integrates cyber and physical security and resilience efforts into an enterprise approach to risk management.

Source: DHS (2013b).

Act is to protect and prevent disclosure of sensitive information related to the risks, vulnerabilities, and events of critical infrastructures. It required trust between the private sector critical infrastructure operators and government agencies because collaboration among stakeholders is instrumental in overcoming the resistance of the private sector to share sensitive information. The current Protected Critical Infrastructure Information program builds on the provisions of this act.

The first National Security Strategy mandated the preparation of the National Infrastructure Protection Plan (NIPP), which was issued in 2006. The current NIPP 2013 (DHS, 2013b) represents an evolution from concepts introduced in the initial version released in 2006 and revised in 2009 (Box 2.11).[26] It provides guidance on efforts of stakeholders to enhance the security and resilience of critical infrastructures across the country in conjunction with national preparedness policy and integrates existing and future critical infrastructure security and resilience efforts into a single national program.

In the United States , as well as countries discussed in the previous sections, the national plan consists of sectoral approaches as mandated by PPD-21. It specifically tasks sector agencies, referred to as sector-specific agencies (SSAs), to lead a collaborative process for critical infrastructure security within each of the 16 critical infrastructure sectors identified within the PPD-21. Each assigned sector agency is responsible for developing and implementing an appropriate sector-specific plan, which details the application of the NIPP concepts to the unique characteristics and conditions of their sector. At the moment of drafting this publication, the SSPs were being updated to reflect new requirements from the NIPP 2013 and published on the official web-page of the U.S. Department of Homeland Security (DHS).[27]

[26] NIPP official web-page, Department of Homeland Security, at: http://www.dhs.gov/national-infrastructure-protection-plan.

[27] For instance, the current sector-specific plan for the communications sector can be found here: http://web.archive.org/web/20141107223442/http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf.

Box 2.12. Main Responsibilities of the Secretary of Homeland Security in Regards to CIIP

In carrying out the responsibilities assigned in HSA 2002, the Secretary of Homeland Security does the following:

- Evaluates national capabilities, opportunities, and challenges in protecting critical infrastructure.
- Analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure.
- Identifies security and resilience functions that are necessary for effective public–private engagement with all critical infrastructure sectors.
- Develops a national plan and metrics in coordination with SSAs and other critical infrastructure partners.
- Integrates and coordinates federal cross-sector security and resilience activities.
- Ascertains and studies key interdependencies among critical infrastructure sectors.
- Reports on the effectiveness of national efforts to strengthen the security and resilience posture of critical infrastructures.

Source: Homeland Security Act of 2002, as amended, http://www.dhs.gov/homeland-security-act-2002.

Governance

In the United States, protection of critical infrastructures is considered to be a shared responsibility among the federal and SLTT entities, along with public and private owners and operators of critical infrastructures. This section outlines the CIIP governance model established at the federal level.

In 2002, the DHS was created, led by the Secretary of Homeland Security.[28] The Secretary is the main authority responsible for providing strategic guidance, promoting a nationwide effort, and coordinating federal activities to encourage the security and resilience of critical infrastructures (Box 2.12). DHS plays a key role within the effort to implement the CIIP framework. Within DHS, the structural unit responsible for CIIP is the National Protection and Programs Directorate. Within this unit, the Office of Infrastructure Protections leads and coordinates national programs and policies on critical infrastructure security and resilience. In addition, the Office of Cybersecurity and Communications is working to prevent or minimize disruptions to CII. Both offices manage around-the-clock monitoring and coordination centers:

- The National Cybersecurity and Communications Integration Center serves as a 24/7 cyber monitoring, incident response, and management center and as a national point of cyber and communications incident integration.[29]
- The National Infrastructure Coordinating Center is the dedicated coordination and information sharing operations center, operating around the clock and maintaining situational awareness of the nation’s critical infrastructure for the federal government.[30]

At the sector level, a significant role within the CIIP governance framework is assigned to SSAs, including preparing and implementing NIPPs and SSPs. The SSAs have institutional knowledge and expertise about the sector, possess familiarity and relationships among the sector actors, and thus also play a critical role in maintaining partnerships and dialoguing with the critical infrastructure operators. The need for SSAs arises from the understanding that each critical infrastructure sector has unique characteristics, operating procedures, and risk profiles. In particular,

[28] Homeland Security Act of 2002, at: http://www.dhs.gov/homeland-security-act-2002.

[29] National Cybersecurity and Communications Integration Center, at: http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.

[30] National Infrastructure Coordinating Center, at: http://www.dhs.gov/national-infrastructure-coordinating-center.

TABLE 2.6. Critical Infrastructure Sector and Assigned Sector Specific Agency (SSA)

Critical infrastructure sector	SSA
Chemical; commercial facilities; communications; critical manufacturing; dams; emergency services; information technology; nuclear reactors, materials, and waste sectors	Department of Homeland Security
Defense industrial base sector	Department of Defense
Energy sector	Department of Energy
Financial services sector	Department of the Treasury
Food and agriculture sector	Department of Agriculture and Department of Health and Human Services
Government facilities sector	Department of Homeland Security and General Services Administration
Healthcare and public health sector	Department of Health and Human Services
Transportation systems sector	Department of Homeland Security and Department of Transportation
Water and wastewater systems sector	Environmental Protection Agency

Source: Sector-Specific Agencies, Department of Homeland Security, at: http://www.dhs.gov/sector-specific-agencies.

SSAs are obliged to carry out the following main roles and responsibilities for their respective sectors:

- Strengthen the security and resilience of critical infrastructure, coordinate with the DHS and other relevant federal departments and agencies, and collaborate with critical infrastructure owners and operators and, where appropriate, with other actors.
- Serve as a day-to-day federal interface for the dynamic prioritization and coordination of sector-specific activities.
- Carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, and regulations.
- Provide, support, or facilitate technical assistance and consultations for the sector to identify vulnerabilities and help mitigate incidents, as appropriate.
- Support the Secretary of Homeland Security's statutorily required reporting requirements by providing sector-specific CII annually.

Assigned SSAs are listed in Table 2.6. DHS continues to play an important role in CIIP not only nationally, but also at the sectoral level. DHS is a dedicated sector-specific agency (SSA) for eight critical infrastructure sectors and is a co-SSA with other agencies for another two critical infrastructure sectors. For instance, the Office of Cyber Security and Communications is the SSA for the Communications and Information Technology sectors, while the Office of Infrastructure Protection is the assigned SSA for another six critical infrastructure sectors.

The National Infrastructure Simulation and Analysis Center (NISAC)[31], commissioned in 2001, supports DHS efforts.[32] The initial objective was "to serve as a source of national competence to address critical infrastructure protection and continuity through support for activities related to counterterrorism, threat assessment, and risk mitigation." Today, the NISAC serves a broad spectrum of objectives within its initial idea to inform decision-making and planning in CIIP (Box 2.13). The Office of Cyber and Infrastructure Analysis within the DHS manages the NISAC.[33]

[31] http://www.sandia.gov/nisac/.

[32] United States Code § 5195c – Critical infrastructures protection, at: https://www.law.cornell.edu/uscode/text/42/5195c.

[33] Office of Cyber and Infrastructure Analysis, at: http://www.dhs.gov/office-cyber-infrastructure-analysis.

Box 2.13. National Infrastructure Simulation and Analysis Center

The NISAC began as a collaboration between Los Alamos and Sandia National Laboratories in 1999 and was incorporated by the United States *Patriot Act* of 2001 into the Department of Homeland Security on its inception in March 2003. The Office of Infrastructure Protection oversees the NISAC's operations.

The NISAC conducts modeling, simulation, and analysis of the nation's critical infrastructures. NISAC analysts assess critical infrastructure risk, vulnerability, interdependencies, and event consequences.

Requests for information or analyses are prioritized and supported by the Homeland Infrastructure Threat and Risk Analysis Center. Joint ventures between the centers are often undertaken to create or advance a needed capability to support multiple governmental decision-makers.

The NISAC plays a vital role under the NIPP, which relies on robust public–private information sharing to protect and build resiliency for the nation's vast infrastructure. The center's multidisciplinary expertise covers the full spectrum of 16 critical infrastructure sectors while focusing on the challenges posed by interdependencies and the consequences of disruption.

NISAC researchers and analysts conduct extensive modeling, simulation, and analysis to support risk mitigation and policy planning. They also provide real-time assistance to DHS decision-makers during such critical incidents as hurricanes, flooding, wildfires, and manmade events.

Source: Authors based on http://www.dhs.gov/about-national-infrastructure-simulation-and-analysis-center and http://www.sandia.gov/nisac/analyses/nisac/.

The departments and agencies listed in Table 2.7 have additional federal responsibilities in specialized or support functions related to critical infrastructure security and resilience that will be carried out by, or along with, other federal departments and independent regulatory agencies, as appropriate.

Observations and Recommendations

When reviewing the international experience in CIIP policymaking and governance, a number of similarities become clear. Different countries arrived at similar solutions while developing national CIIP frameworks, meaning that those solutions proved to be efficient. The authors recommend these standards to countries that are developing their national CIIP frameworks. The following summarizes the findings.

Prioritization of CIIP at the National Level

Preparing and implementing a CIIP framework requires significant involvement of the public and private sector. It requires dedicated financial resources and participation of academia. A significant level of engagement can be achieved by high prioritization of the CIIP agenda at the national level through primary countrywide strategies, such as a national security strategy.

Umbrella Framework for CIIP

CIIP involves many segments and different actors from both the public and private sectors. In those circumstances, a CIIP policy and legal framework would benefit from a single overarching policy document encompassing all related areas and actions, establishing a governance framework, thus creating the full picture of the CIIP framework.

Clear Governance Model for CIIP

CIIP governance at the national level should not be complex. There should be one or only a few policymaking bodies involved at the national level, with clear assignment of sectoral coordination down the line. Each critical infrastructure sector should have its own governance structure that monitors implementation of sector-specific CIIP measures, and coordinates and strengthens

TABLE 2.7. Roles and Responsibilities of Federal Departments and Agencies within the CIIP Framework

Department or agency	Responsibilities
Department of State	Engage foreign governments and international organizations to strengthen the security and resilience of critical infrastructures located outside the United States and to facilitate the overall exchange of best practices and lessons learned.
Department of Justice, including the Federal Bureau of Investigation (FBI)	Lead counterterrorism and counterintelligence investigations and related law enforcement activities across the critical infrastructure sectors. The Department of Justice is authorized to investigate, disrupt, prosecute, and otherwise reduce foreign intelligence, terrorist, and other threats to, and actual or attempted attacks, threats, or sabotage of the critical infrastructure. The FBI also conducts domestic collection, analysis, and dissemination of cyber threat information and is responsible for the operation of the National Cyber Investigative Joint Task Force. This task force serves as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from the DHS, the intelligence community, the Department of Defense, and other agencies.
Department of the Interior	Identify, prioritize, and coordinate the security and resilience efforts for national monuments and icons and incorporate measures to reduce risk to these critical assets, while also promoting their use and enjoyment.
Department of Commerce	Engage private sector, research, academic, and government organizations to improve security for technology and tools related to cyber-based systems. Promote the development of other efforts related to critical infrastructures to enable the timely availability of industrial products, materials, and services to meet homeland security requirements.
Intelligence Community	Use applicable authorities and coordination mechanisms to provide, as appropriate, intelligence assessments regarding threats to critical infrastructures and coordinate on intelligence and other sensitive or proprietary information related to critical infrastructures.
General Services Administration	Provide or support government-wide contracts for critical infrastructure systems and ensure that such contracts include audit rights for the security and resilience of critical infrastructure.
Nuclear Regulatory Commission	Collaborate, as appropriate, on strengthening critical infrastructure security and resilience within competence and sector.
Federal Communications Commission	Partner on: • identifying and prioritizing communications infrastructure; • identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and • working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of communications critical infrastructure.
All federal departments and agencies	Provide information to the Secretary of Homeland Security and the national critical infrastructure centers necessary to support cross-sector analysis and inform the situational awareness capability for critical infrastructures. Classify, prioritize, assess, remediate, and secure their respective internal critical infrastructures that support their primary mission functions. Such infrastructure must be addressed in the plans and execution of the requirements in the National Continuity Policy.[a]

Source: U.S. White House (2013).

[a] "It is the policy of the United States to maintain a comprehensive and effective continuity capability composed of Continuity of Operations and Continuity of Government programs to ensure the preservation of our form of government under the Constitution and the continuing performance of National Essential Functions under all conditions." https://whitehouse.gov1.info/continuity-plan/.

collaboration among critical infrastructure owners and operators.

Dedicated CIP Agency or Dedicated CIP Capacity Within an Existing Body

A CIIP framework covers many critical aspects of national security that involve a broad number of sectors and market actors. Day-to-day operation and maintenance of CIIP requires dedicated attention, and human and financial resources. Many countries found it practical to inaugurate a national CIP-dedicated agency to handle this work. Others established dedicated capabilities within existing institutions. Despite the modalities, each country that takes CIIP seriously had to increase its administrative and operational capacity dedicated to CIIP.

Regulations

CIIP regulations should set standards for the security of critical infrastructures and requirements for restoration and recovery after emergency situations. Regulations should be addressed with critical infrastructure operators, who should design schemes to monitor particularly vulnerable critical infrastructure sites. An important objective of regulations is to set up a mechanism to report security incidents to competent authorities, usually a national Computer Emergency Response Team. Instead of bans and restrictions, it is better to get critical infrastructure operators to realize the benefits of including resilience thinking throughout their organizations and asset planning, from physical design to operational procedures and contingency planning. Lost revenue, reputational damage, contractual penalties, and the potential for litigation are strong drivers for managing risks and building resilience.

3

Determining and Identifying Critical Infrastructures

What Is Critical Infrastructure?

Determining and identifying critical infrastructure assets that must be protected is the first step toward improving national critical information infrastructure protection (CIIP). The Institute of Civil Engineers has defined critical infrastructures as those that are especially important for the system as a whole or for other infrastructures (ICE, 2009). A more explicit definition refers to critical infrastructure as organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences (Germany, 2009). Wordings of definitions vary from country to country, but overall, the objective is to capture those infrastructure assets that could be linked to the vital functions of the society and economy and where failure could have significant negative impact on both. Box 3.1 reviews some definitions of critical infrastructure.

In this regard, the definition of critical infrastructure is close to the description of economic infrastructure. The World Economic Forum (WEF) defined economic infrastructure as assets that generate growth and enable society to function. In 2014, this definition was expanded to include assets that enable society and the economy to function. Examples include strategic infrastructure such as transport facilities (air, sea, and land), utilities (water distribution networks, gas pipelines, electricity grids, and electrical power generation), flood defenses, waste management, and telecommunications networks (WEF, 2012). In turn, economic infrastructure is sometimes regarded as part of the strategic infrastructure.

Apart from critical infrastructure, critical information infrastructure (CII) is related directly to information and communications technology (ICT) and CIIP relates to protection from cyberattacks. CII is a part of critical infrastructure and both sub-jects are interconnected (Box 3.2).

Identifying Critical Infrastructures

Water, energy, and transport are among the common critical infrastructure sectors for most countries. But the full set of critical infrastructure sectors varies depending on the specifics of the national situation in a particular country, including its economic dependencies and supply chains. Particular sectors could become critical (or not) depending on the existence (or not) of risks that could threaten its operation. This book outlines the situations in selected countries and demonstrates the differences. What is critical at the national level is determined by risk assessments that allow decision-makers to understand existing risks (internal and external) to the

Box 3.1. Definitions of Critical Infrastructure

All critical infrastructure definitions recognize the vital and indispensable importance of the service or function provided by the asset to the society. Most countries define infrastructure as critical if its disruption would have a nationwide impact. However, the subject of impact varies slightly from country to country. For instance, in the United States, the impact of critical infrastructure disruption is closely linked to the safety and security of citizens and the economy. In the EU, the region-wide definition includes the economic and social wellbeing of people. The definition from the North Atlantic Treaty Organization (NATO) also includes any impact on the environment. The following are definitions of critical infrastructure from various entities.

International Organization for Standardization: Organizations and facilities that are essential to the functioning of society and the economy as a whole. The standard elaborates that a failure or malfunction of such organizations or facilities would result in sustained supply shortfalls, make a significant impact on public security, and have other wide ranging impacts.

International Telecommunication Union: The key systems, services, and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of these.

NATO: Physical or virtual systems and assets under the jurisdiction of a state that are so vital that their incapacitation or destruction may debilitate a state's security, economy, public health or safety, or the environment.

EU: An asset, system, or part thereof located in a member state that is essential to vital societal functions, health, safety, security, economic, or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a member state as a result of the failure to maintain those functions.

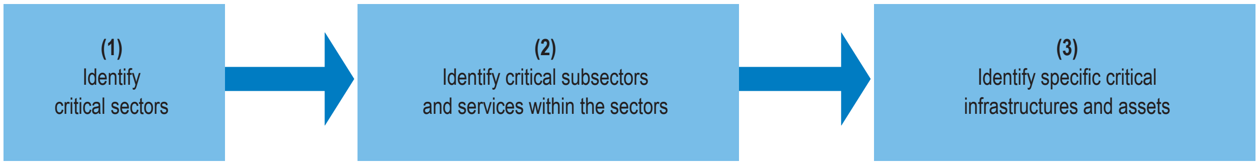
United States: The assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Source: Authors; EU (2008); ISO (2013); ITU (2008); Richardson (2008); Schmidt (2013).

country and how they are linked to essential services and infrastructure in terms of impact. As outlined by the Joint Research Center, the research arm of the European Commission, effective risk assessment methodologies are the cornerstone of a successful CIIP program. Risk assessment is indispensable to identifying threats, assesing vulnerabilities, and evaluating the impact on assets, infrastructures, or systems, taking into account the probability of the occurrence of these threats (Giannopoulos, Filippini, and Schimmer, 2012). Consequently, the evaluation identifies not only *what* should be protected, but also *from what threats* and *what level of effort* is required. There are conventional risk assessment methodologies that are currently used.

Practically, however, one of the main constraints to identifying critical infrastructure is limited knowledge and thus a lack of clarity for appropriate input data for any risk assessment. In particular, among the developing countries, the knowledge about location, nature, condition, and impact of threats related to a system's failure, climate change, or terrorism is immensely limited. Identifying critical infrastructures and particular assets within critical sectors is thus a complicated task that requires time, a systematic approach, and good collaboration with and within potential critical infrastructure sectors. Preparing datasets of assets within particular networks or sectors provides a better understanding of total infrastructure,

FIGURE 3.1. Identifying Critical Sectors and Infrastructures


(1)
Identify
critical sectors
(2)
Identify critical subsectors
and services within the sectors
(3)
Identify specific critical
infrastructures and assets

Source: ENISA (2015).

which naturally includes infrastructure that needs to be identified as critical. In other words, a dataset offers a full picture of the situation and is a useful tool for supervision. As knowledge of critical infrastructures and related expertise advance, the accuracy of identification increases accordingly, and thus each subsequent round of CIIP activities becomes increasingly more accurate and specific.

As such, critical infrastructure identification could be visualized as a three-step process (Figure 3.1):

1. Identify critical infrastructure sectors
2. Identify critical infrastructure subsectors and services
3. Identify specific critical infrastructures and assets

Despite the visual simplicity, the major challenge within this process is in the last stage. There is no single methodology to identify specific critical infrastructures and assets. Those that are currently applied are sector-specific because of the differences and complexities of individual sectors. There are no common metrics to identify critical infrastructures that could be applied across sectors. For example, the health sector completely differs from the financial sector, chemical industry, or ICT sector.

It is highly unlikely that a common methodology and common criteria could be developed for all sectors. For 10 specific critical infrastructure sectors, 10 parallel asset identification processes, each with its own methodology, approach, details, and timeline, are necessary. Not to mention that sectoral interdependencies is another important parameter that should be taken into account within each critical infrastructure sector as it affects sectoral CIIP methodologies and plans (Min et al., 2009) (Box 3.2).

Recently interdependencies are increasingly being studied by different countries. For instance, there is an initiative to explore the interdependencies between the ICT and energy sectors because of their increasing convergence.[1] The impact of cyber threats on different critical infrastructure sectors is another interdependency that currently is highly relevant. Cyber security incidents are a major concern and are perpetual threats to CII (Buldyrev et al., 2010) and, in particular, to Supervisory Control and Data Acquisition (SCADA) systems. Distinguishing vulnerable elements that could be impaired by cyber-attacks has to be performed in the CII identification process.

Governance and research bodies dedicated to critical infrastructure protection (CIP) around the world are putting significant effort into developing and researching methodologies and techniques to identify critical infrastructure. Despite considerable progress, there is additional work to be done. In that context, the need to involve domestic academia and research bodies cannot be overemphasized.

The sections that follow expand on the practices used by the selected countries to identify critical infrastructure. Although it is not possible to describe the methodologies used by each country

[1] Cyber Security was the agenda of the Thematic Network on Critical Energy Infrastructure Protection (TNCEIP) in 2011; TNCEIP was established by DG ENERGY (structural unit of the European Commission of the EU); http://ec.europa.eu/dgs/energy/newsletter/dg/2012/0119newsletter.html.

Box 3.2. Interdependencies of Critical Infrastructures

Four types of interdependencies are identified for critical infrastructures:

Physical: The operation of one infrastructure depends on the material output of the other.

Cyber: Dependency on information transmitted through the information infrastructure.

Geographic: Dependency on local environment that simultaneously affects several infrastructures.

Logical: Any kind of dependency not characterized as physical, cyber, or geographic.

Besides cross-sectoral interdependencies (e.g., ICT and electricity, satellite navigation, and transport), in Europe, intra-sectoral interdependencies of national infrastructures that form the European infrastructures can be identified. For instance, the high-voltage electricity grid of the EU, which comprises the interconnected national high-voltage electricity grids.

Source: Giannopoulos, Filippini, and Schimmer (2012).

in great detail, this book provides a conception of what metrics may be relevant to the process, definitions adopted by the countries, and what sectors were classified as critical.

European Union

Global threats and the disastrous events previously faced by the EU accelerated the advance in CIIP. The EU has defined the meaning of critical infrastructure, has identified sectors and assets, and has initiated important programs, such as the European Programme for Critical Infrastructure Protection (EPCIP). See *CIIP Policy and Governance in the EU* in Chapter 2.

The EPCIP (European Communities, 2006) defined critical infrastructure as those assets of the highest importance for the community and that, if disrupted or destroyed, would affect two or more member states or a single member state if the critical infrastructure is located in another member state. This definition includes trans-boundary effects resulting from interdependencies between interconnected infrastructures across various sectors. Formally, the critical infrastructure definition is introduced within the European CIP directive as follows:

> Critical infrastructure: an asset, system or part thereof located in Member States that is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact on a Member State as a result of the failure to maintain those functions (European Communities, 2006).

It is important to note that EU-level critical infrastructure consists of infrastructure located in member states whereby its disruption or destruction would have a significant impact on at least two member states. The European CIP Directive (EU, 2008) provides a list of 11 critical infrastructure sectors (Table 3.1).

The EU uses sectoral criteria to identify critical infrastructure. Criteria are provided in the European Certification of Informatics Professionals document on the basis of the severity of the consequences of disruption or destruction, which is assessed based on the:

- Public effect (percentage of population affected)

TABLE 3.1. Critical Infrastructure Sectors Identified by the EU CIP Directive

1.	Energy
2.	Nuclear industry
3.	Information communication technologies
4.	Water
5.	Food
6.	Health
7.	Financial
8.	Transport
9.	Chemical industry
10.	Space
11.	Research facilities

Source: EU(2008).

- Economic effect (significance of economic loss and/or degradation of products or services)
- Environmental effect
- Political effect
- Psychological effect

Member states are tasked with identifying those infrastructures that satisfy these criteria. The absolute value for the threshold for each criterion may vary, and it is the prerogative of each member state to specify it. For example, the impact on the economy or on the portion of population may be different depending on the size of the country or composition of the economy. The energy, transport, and ICT sectors are considered to be critical at the EU level. Specific subsectors are already identified for energy and transport (Table 3.2); however, identifying subsectors for ICT is still in progress because of the sector's complexity. The European Agency for Network and Information Security (ENISA) is tasked with this work.

To facilitate a cooperative approach, the relevant member states—those within which European Critical Infrastructures (ECI) are identified and those that may be affected by its disruption—are negotiating the designation of ECIs. Once an ECI is identified, a specific set of actions are taken by its owners/operators to develop an Operator Security Plan that documents the critical assets and security measures. Concessions do exist for ECI entities that already have similar or equivalent requirements in place.

The CIP Directive empowers the authorities in member states to be in charge of ensuring that ECIs comply with its requirements. Each country's government chooses which particular authority or authorities are responsible for transposing and/or implementing the CIP framework. The member state is accountable for properly transposing the EU-level provisions into their national legislation. To facilitate collaboration among member states, the EU organized various groups to create a platform to exchange information, experiences, and planning. For example, the Commission on the EPCIP facilitated an integrated approach by creating the CIP Contact Group. This group, which is chaired by the European Commission, brings together the CIP Contact Points from each member state. Each member state appoints a Contact Point who coordinates CIP issues within the member state and with other member states, the European Council, and the Commission. Any other authorities in the member state may also be involved in CIP issues.

In 2014, ENISA reviewed lists of national critical infrastructure, associated subsectors, and services

TABLE 3.2. Subsectors of Energy and Transport Identified at the EU Level

Sector	Subsectors
Energy	• Electricity (infrastructures and facilities to generate and transmit electricity) • Gas (production, refining, treatment, storage, and transmission by pipelines; LNG terminals) • Oil (production, refining, treatment, storage, and transmission by pipelines)
Transport	• Roads • Rail • Air • Inland waterways • Ocean and short-sea shipping and ports

Source: EU (2008).

adopted by the member states. It then suggested a reference list to be used in the initial stage of member states reviewing the sectors and services they may classify as critical at the national level (Appendix 1). The list is not mandatory but can be analyzed and adapted by each country based on differences in critical infrastructure sectors, subsectors, and risks.

As a region, the EU's considerable effort in protecting critical infrastructures is an example of best practices of a well-developed systematic approach. For example, notable results have been achieved in sectoral criteria to identify critical infrastructure. The process of identifying European critical infrastructures resulted in security and resilience measures through Operator Security Plans. Currently, the EU is reviewing the CIP Directive to identify additional European critical infrastructure sectors.

Finland

Finland has a highly industrialized, largely free-market economy that depends on technology industries such as mechanical engineering, information technology (IT), telecommunications, and electronics, as well as metals and forestry. Fifty percent of total Finnish exports are from the technology industry (Technology Industries, 2014). The industrial sector generates over 25 percent of Finland's gross domestic product and ICT's share remains over 10 percent (IMF, 2014). This very quick look demonstrates the dependency of the Finnish economy on the technologies and industrial sectors. Consequently, any disruptions to those essential sectors could result in dramatic consequences for the Finnish economy.

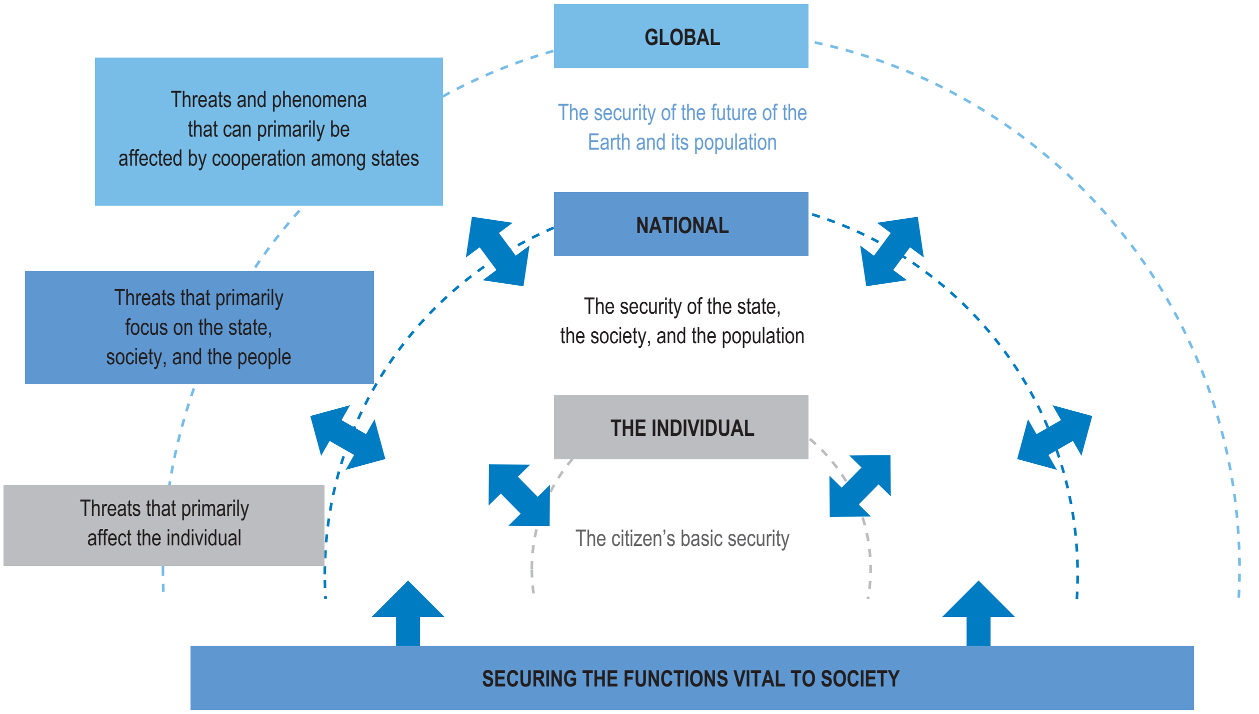
Finland has defined CIIP as an objective to ensure the continuity of production and infrastructure vital to society under all circumstances in such a way that the living conditions of the population and the critical functions of society are secured in the event of disruptions and emergencies, including a state of defense. Finland aims to safeguard national sovereignty and their citizenry's ability to function in all circumstances by securing vital operations such as state leadership, the external capacity to act, military defense, internal security, the economy, and society, maintaining the livelihood of the population. See *CIIP Policy and Governance in Finland* in Chapter 2.

For threats analysis, Finland uses a generic threat scenario (Figure 3.2). A threat scenario is a general description of disturbances in the security environment which, should they materialize, could jeopardize the security of society, the livelihood of the population, or the sovereignty of the state.

Finland has identified nine critical infrastructure sectors (Table 3.3). According to Finnish Security and Defense Policy (Finland, 2004), ICT was identified as one of the critical infrastructure sectors because cyber security threats are increasingly targeting national critical infrastructures. ICTs are used by the majority of government agencies, security authorities, and vital industries. Identification of ICT as one of the critical infrastructures leads to higher security standards for constructing communication networks and data systems.

In its CIIP approach, Finland is more focused on critical infrastructure resilience than protection. Having an economy that largely depends on the ICT industry, the Finnish CIIP strategy puts significant emphasis on cyber security threats. Numerous measures, including a strong Computer Emergency Response Team, are in place to safeguard critical infrastructures from cyber-attacks. An extensive knowledge base, strong expertise, a long tradition of close public–private cooperation, and cross-sector collaboration are cornerstones of Finland's approach to resilient cyberspace. Investments in technical and organizational measures to strengthen cyber security resulted in fewer infected computers, earlier detection of malicious network activities using sophisticated tools and sensors, and comprehensive reporting and investigation of security incidents. According to experts, Finland enjoys the most secure cyberspace in the world (Microsoft, 2014).

FIGURE 3.2. Finland's Threats-Based Approach to CIIP


GLOBAL
The security of the future of the Earth and its population
Threats and phenomena that can primarily be affected by cooperation among states
NATIONAL
The security of the state, the society, and the population
Threats that primarily focus on the state, society, and the people
THE INDIVIDUAL
The citizen's basic security
Threats that primarily affect the individual
SECURING THE FUNCTIONS VITAL TO SOCIETY

Source: Finland (2006a).

TABLE 3.3 Critical Infrastructure Sectors in Finland

1. Energy networks and supply
2. ICT, including networks, SCADA, and payment systems
3. Transportation and logistics systems
4. Water supply and other municipal utilities
5. Infrastructure construction and maintenance
6. Financial services
7. Food supply
8. Health services
9. Media

Source: Finland (2006).

United Kingdom

The UK's advanced infrastructure enhances its national productivity and global competitiveness, allowing businesses to grow and enabling them to reach suppliers and deepen labor and product markets. In 2014, the UK's National Infrastructure Plan set out an ambitious infrastructure vision for £460 billion of planned public and private investment (which includes oil and gas investment) (Atkins, 2015). To achieve and protect those investments, the government maintains high safety and security standards for infrastructure.

The UK identifies terrorism, espionage, and cyber-attacks as the main threats to national critical infrastructures. Those threats could materialize individually or in combination, whereby significant threats could come from international terrorist acts combining mass casualties with substantial disruption to vital services such as energy, transport, and communications (CPNI, 2010). The country considers both traditional and cyber espionage threats to UK interests, with the commercial sector being very much on the front line. In today's high-tech world, interest has moved toward intellectual property in communications, IT, genetics, aviation, electronics, and many other industries. The risk of industrial cyber espionage, in which one company actively attacks another through cyberspace to acquire high value information, is real.

The UK aims to protect its critical infrastructures using a combination of physical, information, and personnel security measures. Physical security measures aim to either prevent a direct assault on premises or reduce the potential damage and injuries that can be inflicted should an incident occur. Personnel security is a system of policies and procedures that seek to manage the risk of staff (permanent, temporary, or contract) exploiting, or intending to exploit, their legitimate access to an organization's assets or premises for unauthorized purposes. Almost all critical industrial infrastructures and processes are managed remotely from central control rooms, using various forms of process control and SCADA technology. The UK understands and mitigates electronic attack risks to SCADA systems and facilitates this effort through a focused program of CIIP.

The UK's critical infrastructure is defined as those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services on which the UK relies, the loss or compromise of which would lead to severe economic or social consequences such as loss of life. Infrastructure sectors identified as critical are listed in Table 3.4. Assets within the critical infrastructures are identified as critical using a Criticality Scale, which assigns categories for different degrees of severity of impact (Box 3.3). These assets are called Key Points.

Splitting critical infrastructure sectors into subsectors allows for better organization of CIIP implementation. For example, the communications sector is split into data communications, fixed voice communications, mail, public information, and wireless communications. Emergency services is subdivided into ambulance, fire, and rescue, and includes the coastguard and police. And, the energy sector is divided into electricity, natural gas, and petroleum, among others.

The UK's approach to CIIP puts particular emphasis on terrorism threats. The threat of industrial cyber espionage is another particularity of the UK's CIIP framework. In other countries, greater emphasis is being placed on the cyber security aspects of CIIP.

TABLE 3.4. Critical Infrastructure Sectors in the UK

1. Energy
2. Communications
3. Emergency services
4. Financial services
5. Food
6. Government
7. Health
8. Transport
9. Water

Source: CPNI, at: http://www.cpni.gov.uk/about/cni/.

Spain

Spanish critical infrastructure sectors were not explicitly defined until 2007 when the State Security Secretariat approved the National Plan for the Protection of Critical Infrastructures (see *CIIP Policy and Governance in Spain* in Chapter 2). The plan defines critical infrastructures in relation to threats, and Spain is particularity dedicated to the security of its cyberspace. To this end, the National Cyber Security Strategy (Spain, 2013b) targets CIIP by strengthening prevention, defense, detection, and response capabilities vis-à-vis cyber-attacks.

Spain defines critical infrastructure as "those installations, networks, services, physical equipment, and information technologies whose interruption or destruction would have a grave impact on the health, security, or economic wellbeing of the citizens or on the efficient functioning of the state institutions and of the public administration" (Spain, 2007). Critical infrastructure includes a list of 12 strategically critical sectors (Table 3.5).

In 2007, the government issued a catalog with an exhaustive list of national critical infrastructures. This classified catalog contains around 3,500 critical installations all over the country. The catalog is a living document that is periodically updated. These sensitive facilities include power grids and plants, communications, finance, healthcare, food, water storage, water treatment, and water networks, airports, ports, national monuments, and the production, storage, and transportation of

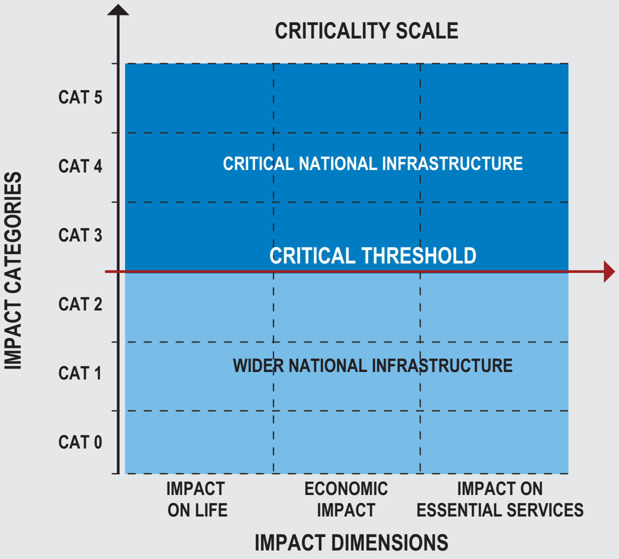
Box 3.3. Criticality Scale Used in the UK

Infrastructure is categorized according to its value or "criticality" and the impact of its loss. This categorization is done using the Criticality Scale, which assigns categories for different degrees of severity of impact.

Not everything within a national infrastructure sector (the UK has identified nine critical infrastructure sectors) is critical. Within the sectors there are certain critical elements of infrastructure, referred to as Key Points, the loss or compromise of which would have a major detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life. These critical assets make up the nation's critical national infrastructure and are referred to individually as infrastructure assets. Infrastructure assets may be physical (e.g., sites, installations, or pieces of equipment) or logical (e.g., information networks or systems).

The Criticality Scale includes three dimensions:

FIGURE 3.3. The Three Dimensions of the Criticality Scale



1. Impact on delivery of the nation's essential services
2. Economic impact arising from the loss of an essential service
3. Impact on life arising from the loss of an essential service

The Centre for the Protection of National Infrastructure (CPNI) developed an impact-driven, vulnerability-focused, and threat-informed approach, which rates each Key Point on a Criticality Scale in the event of its loss. This scale rates the impact of each Key Point on a scale of 5 down to zero. Sector significance and impact on the UK population are key considerations in determining the rating of an event when applying this scale:

Category 5: catastrophic events

Category 4: severe events

Category 3: substantial events

Category 2: significant events

Category 1: moderate events

Category 0: minor events, with no impact on any sector

Once each Key Point is rated, CPNI provides security advice for its protection, which is then implemented by the sponsor government department. For example, aviation falls under the Department of Transport.

Source: Authors based on CPNI, at: http://www.cpni.gov.uk/about/cni/#sthash.kUx3205S.dpuf; UK (2010b).

TABLE 3.5. Critical Infrastructure Sectors in Spain

1. Chemical industry
2. Nuclear industry
3. Investigative installations
4. Centers of power
5. Space
6. Energy
7. Telecommunications
8. Transportation
9. Water supply
10. Alimentation
11. Financial services
12. Public health

Source: National Center for the Protection of Critical Infrastructure.

TABLE 3.6. Critical Infrastructure Sectors in Korea

1. Energy
2. Telecommunications
3. Transportation
4. Financial services
5. Health and medical services
6. Nuclear energy
7. Environment
8. Government critical facilities
9. Water supply

Source: Korea (2010).

dangerous goods, such as chemical, biological, and nuclear materials.

The criteria for including such facilities in the catalog is a mix of factors: range, scale and temporal effects and parameters, damage, economic impact, and effect on essential services. The catalog is classified given its high sensitivity with regards to national security.

Spain is a good example of a relatively recent, rapidly advanced and adopted CIIP framework. The major effort occurred between 2007 and 2013. The country adopted a CIIP strategy, designed plans, emphasized cyber security threats, and created a catalog with an exhaustive list of the national critical infrastructure assets. Now Spain concentrates on implementing and further improving its critical infrastructures.

Korea

Korea's CIP Law defines national critical infrastructure as "designated facilities deemed necessary to be continuously managed to protect the national backbone systems" (Korea, 2010). Table 3.6 provides a list of Korea's nine critical sectors. Some infrastructure facilities, such as telecommunications, can be designated as both critical infrastructure and critical information infrastructure based on different laws.

The Korean economy depends heavily on international trade. In 2013, Korea was the eighth largest exporter and seventh largest importer in the world due to its highly developed electronics, motor vehicle, and heavy industries. The national ICT infrastructure plays a crucial role in providing public safety and stable services that are essential for everyday life. Following the cyber-attacks in 2013, whereby government, news media, television stations, and bank websites were compromised, the government committed to stronger defense of cyberspace. The following details the process by which CII is identified and designated that was recently put in place.

All ICT systems related to infrastructure that could have a serious impact on national security and the daily lives of citizens and the economy in the event of a cyber incident are designated critical infrastructure. Those include ICT infrastructures that the government, public agencies, or the private sector operate and manage, as shown in Table 3.7.

There are 354 ICT infrastructures that were designated as CII in 2015. They are run by 17 relevant central administrative agencies and 209 management organizations.

When there is a facility whose importance is recognized by the Ministry of Science, ICT, and Future Planning (MSIP) or the National Intelligence Service (NIS),[2] the relevant central administrative agency asks the management organization for a designation appraisal. The relevant central administrative agency provides information such as evaluation methods for infrastructure designation and detailed criteria for designation.

[2] See also *CIIP Policy and Governance in Korea* in Chapter 2.

TABLE 3.7. CII within Critical Infrastructure Sectors in Korea

Critical infrastructure sector	Critical information infrastructure
Administration	National information service network; internet and operation systems used by local governments
Finance	Internet banking system; cyber trading system operated by securities businesses
Communications	Internet-connected networks, IDC, VoIP, and IPTV service
Energy	Power generation control and supervision system; power transmission SCADA system
Water supply	Piped water supply purification and control system
Medical services	Health insurance management system; hospital information system
Transportation	Flight/voyage information management system; comprehensive railroad control system
Others	Election-related information / communications system; National Pension Management System

Source: Korea (2010).

The management organization evaluates whether it can be designated as CII. The relevant central administrative agency then confirms the results of the management organization's evaluation in consultation with experts that form the Committee for the Protection of Information Infrastructure (CPII) and assistance from the Working-Level Committee. CPII then makes the final decision. After the given infrastructure is judged as requiring designation as CII, the relevant central administrative agency gives a designation notice to the management organization. The management organization installs a protection system, including vulnerability analysis. The central administrative agency then posts a notice on the official gazette. The process of CII designation is presented in Figure 3.4.

The designated CII's management organization is required to establish protective measures every year to find and eliminate new vulnerabilities from a short-term perspective and must implement an effective management system by analyzing the ripple effects from long-term incidents.

The management organizations of designated infrastructures should carry out activities to strengthen infrastructure protection. Such activities are typically in three stages:

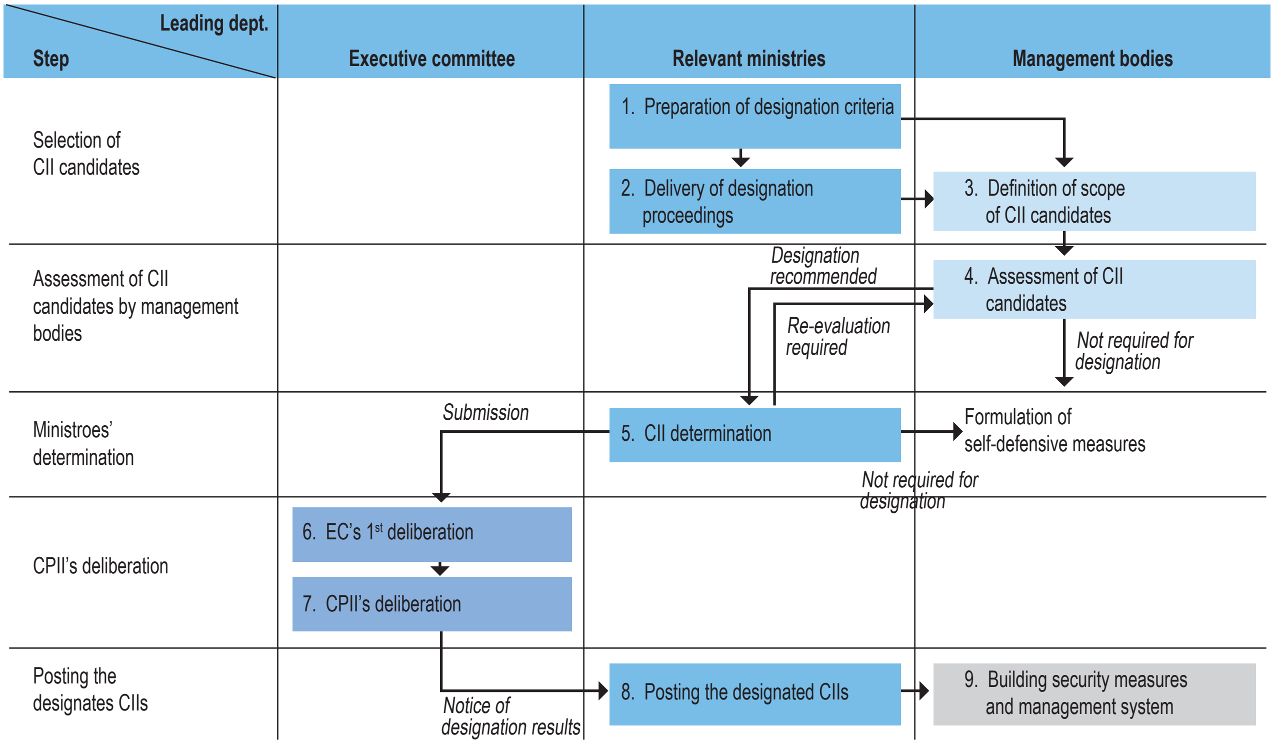
1. Analyze and appraise vulnerability
2. Devise a protection plan
3. Confirm protective measures have been carried out

Table 3.8 shows the administrative, physical, and technical aspects of a vulnerability analysis. The assets that require vulnerability analysis include information and control systems. If there are other systems linked with CII, the influence of the linked system on the infrastructure is also included. The management organization should select major vulnerabilities discovered during the analysis and appraisal, and enter improvements into the subsequent year's detailed tasks for protective measures. Such detailed tasks are divided into prevention and rehabilitation plans. The prevention plan focuses on items targeted for improvement based on the results of the vulnerability check for incident prevention; the rehabilitation plan concentrates on forming a system to deal with incidents and crisis situations.

United States

The United State's critical infrastructures are diverse and complex. In the past, the systems and networks of the infrastructures were physically and logically independent and separate. With advances in technology, the systems within each sector became automated and interlinked through computers and communications facilities. Interdependent and interrelated infrastructure

FIGURE 3.4. **Process of Identifying and Designating CII**


Leading dept.
Step
Executive committee
Relevant ministries
Management bodies
Selection of CII candidates
Assessment of CII candidates by management bodies
Ministroes' determination
CPII's deliberation
Posting the designates CIIs
1. Preparation of designation criteria
2. Delivery of designation proceedings
3. Definition of scope of CII candidates
Designation recommended
4. Assessment of CII candidates
Re-evaluation required
Not required for designation
Submission
5. CII determination
Formulation of self-defensive measures
Not required for designation
6. EC's 1st deliberation
7. CPII's deliberation
8. Posting the designated CIIs
Notice of designation results
9. Building security measures and management system

EC: Executive Committe
CPII: Committe on the Protection of II

Source: Finland (2006).

TABLE 3.8. **Details of a Vulnerability Analysis**

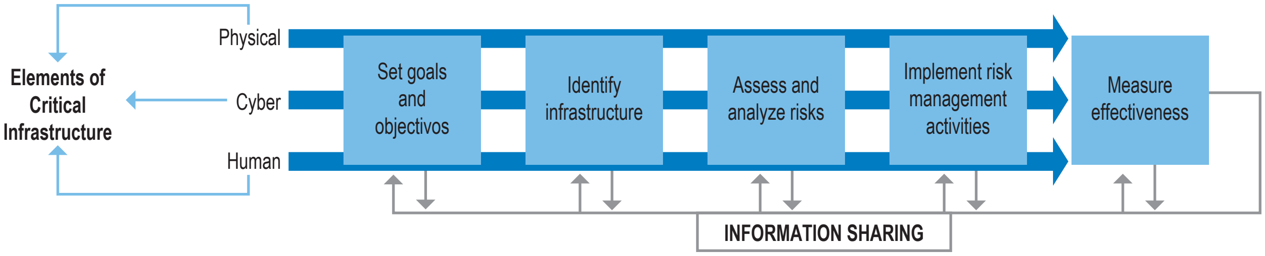
Vulnerability	Details
Management-related	Exposure in information security policy formulation and management; information security organization and human resources security; and information security awareness and education and training.
Physical	Improper access control to the CII; installation of support facilities (e.g., power sources and firefighting facilities).
Technological	Weaknesses with unauthorized access to systems; vulnerability in information leaks and alteration; and delays in services and service failures.

Source: MSIP Notice No. 2013–37.

is more vulnerable to physical and cyber disruptions because it has become a complex system with single points of failure. The elements of critical infrastructure themselves are also considered possible targets of terrorism. The authors selected the United State's best practices to be investigated herein because of the advanced work on CIP since national attempts at protection started in 1998, much before any other country.

The United State defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters" (DHS, 2013a). The government's CIIP policy mission is to strengthen the security and resilience of the nation's critical infrastructure by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure community (DHS, 2013b). The current list of 16 critical infrastructure sectors

FIGURE 3.5. Critical Infrastructure Identification Framework



Source: DHS (2013b).

was established in 2013 (U.S. White House, 2013) (Table 3.9).

The government's effort to identify critical infrastructure is based on a phased approach (Figure 3.5). Three risk factors are considered throughout the process: physical, cyber, and human. This is similar to the UK, which considers physical, information, and personnel security, and to Korea, which looks at management-related, physical, and technological factors.

The U.S. federal government identifies and prioritizes nationally significant critical infrastructure based on the statutory definition and national considerations. Infrastructure owners and operators identify assets, systems, and networks that are essential to their continued operations and delivery of products and services to customers. At the sector level, institutions collaborate with owners and operators to develop lists of infrastructure that are significant at the national, regional, and local levels.

The method of collecting critical infrastructure assets from the municipal level and placing it on the national critical infrastructure list has had its weaknesses. In 2006, the U.S. infrastructure list included about 77,000 assets and it was not manageable. Therefore the approach was changed to use more stringent criteria for critical infrastructure selection (such as higher thresholds) to reduce the list to several thousand assets.

TABLE 3.9. Critical Infrastructure Sectors in the United States

1.	Chemical
2.	Commercial facilities
3.	Communications
4.	Critical manufacturing
5.	Dams
6.	Defense industrial base
7.	Emergency services
8.	Energy, including the production, refining, storage, and distribution of oil and gas, and electric power (except for commercial nuclear power facilities)
9.	Financial services
10.	Agriculture and food
11.	Government facilities
12.	Public health and healthcare
13.	Informat ion technology
14.	Nuclear reactors, materials, and waste
15.	Transportation systems (including mass transit, aviation, maritime, ground / surface, and rail and pipeline systems)
16.	Water and wastewater systems

Source: U.S. White House (2013).

Observations and Recommendations Regarding Defining and Identifying Critical Infrastructure

Definition of critical infrastructure: Defining critical infrastructure is the first step toward identifying critical infrastructures as it creates metrics that can be used later to designate critical infrastructures. Most of the definitions include the impact of a disruption as one of the metrics. The size of impact is usually defined as nationwide. Another metric is the subject of disruption, which slightly varies from country to country. Moreover, the traditional understanding of security (physical) is generally broadened to include economic security.

TABLE 3.10. Critical Infrastructure Sectors by Country

Critical infrastructure sectors	EU	United States	Finland	UK	Spain	Korea
Energy	**+**	**+**	**+**	**+**	**+**	**+**
Transport	**+**	**+**	**+**	**+**	**+**	**+**
ICT and (tele)communications	**+**	**+**	**+**	**+**	**+**	**+**
Financial	**+**	**+**	**+**	**+**	**+**	**+**
Water	**+**	**+**	**+**	**+**	**+**	**+**
Health	**+**	**+**	**+**	**+**	**+**	**+**
Food	+	+	+	+	+	
Government facilities		+		+		+
Chemical	+	+			+	
Nuclear	+	+			+	+
Emergency services		+		+		
Research	+				+	
Space	+				+	
Critical manufacturing and power centres		+			+	
Dams		+				
Commercial facilities		+				
Defence industry		+				
Media			+			
Infrastructure maintenance			+			
Environment						+
Total:	**11**	**16**	**9**	**9**	**12**	**9**

Source: Authors.
Note: In bold are sectors that are considered critical infrastructure in all the countries studied.

Risk assessment: Identifying critical infrastructures starts with a risk assessment at the national level. The aim of the assessment is to understand the risks to national security, including economic security and citizen wellbeing. There are well-recognized methodologies that can be used for a risk assessment.

Identify critical infrastructures: After risks are known, an analysis is required to understand links between those risks and national infrastructures. The analysis should include risk tolerance per infrastructure and per service, which will enable the definition of critical infrastructure sectors, subsectors, and assets within critical infrastructures. Those assets will compose the list of national critical infrastructures.

List of identified critical infrastructure assets: Information about all the identified critical infrastructure assets should be stored in a centralized list. This information is usually classified. It is important to ensure that a national critical infrastructure list includes information about all critical infrastructure of national importance. Critical infrastructures that are identified at sub-national levels and that are not of strictly national importance could be listed within the sub-national lists.

List of critical infrastructure sectors: Composition of the critical infrastructure sector list will vary from country to country depending on the national circumstances (Table 3.10). There are six sectors that were considered critical infrastructure sectors in all the reviewed countries and the EU (bold in Table 3.10) and it is likely that these sectors will compose the critical infrastructure sector lists in Latin American and Caribbean countries as well.

4

Protection: Methods and Forms of Implementation

The previous chapters elaborated the policy and legal frameworks that comprise the basic steps to creating a critical information infrastructure protection (CIIP) framework. They also reviewed governance models, critical infrastructure assignment processes, and the selection of assets within critical infrastructure sectors. These chapters also considered the risks that those infrastructures are susceptible to and risk tolerance levels in each case. Such preparatory work allows countermeasures (or protection measures) to be formulated to safeguard critical infrastructures. The next step is to implement the protection and resilience design.

Ultimately, CIIP implementation is an effort of all the parties involved: the public sector, the private sector, and public–private partnerships (PPP). Critical infrastructure cannot be protected in isolation and joint efforts multiply the level of its defense. This chapter is dedicated to understanding implementation of CIIP.

Public Sector Approaches

Responsibility for developing and coordinating CIIP policy rests first and foremost with the national government. Because of the importance of national security at the political level, the leading authority on CIIP should be assigned to the entity in charge of national security and the relevant ministries for internal affairs at strategic implementation. For instance, in the United States, the Secretary of Homeland Security leads CIIP at the political level and the Department of the Homeland Security (the line ministry for internal affairs) coordinates strategic implementation. In Spain, the political level authority is the Secretary for Security of State and the line ministry supports the implementation process. In the UK, the governmental structure that decides on issues related to CIIP is the Cabinet Office. The Cabinet Office:

- Develops and coordinates the CIIP framework;
- Enacts a transparent and clear governance framework;
- Mandates clear authority at the political and strategic levels;
- Provides political support to the legislative side of CIIP framework enhancement;
- Supports implementation, regular review, and adjustment of the CIIP policy; and
- Ensures adequate budgeting to implement the CIIP policy, including human resources and planned activities.

At the technical level, countries mostly rely on dedicated CIIP implementation bodies. For the purpose of this study, the authors use the term National CIP Agencies (NCIPA), which are institutions tasked with CIIP and that play a leading role in all activities related to selecting and protecting critical infrastructures. Depending on their mandate, which can vary from country to country, they are involved in:

- Improving secondary legislation related to CIIP;
- Supervising the implementation of relevant legislation by the involved parties;
- Auditing security plans of critical infrastructure operators;
- Advising critical infrastructure operators, sharing information, disseminating alerts on security threats, and supporting efforts for CIP and resilience; and
- Organizing joint exercises to test procedures and strengthen relationships and cooperation habits.

Collaboration among NCIPAs and critical infrastructure operators is another key policy issue. Strong cooperation, which considers joint efforts from both sides, is a prerequisite for successful implementation of any CIIP-related initiatives and programs. For example, to supervise and monitor CIIP situations, NCIPAs need to receive information from critical infrastructure operators. In turn, consolidated feedback from NCIPAs based on the information provided, including threat awareness and recommendations, is important and necessary for critical infrastructure operators to secure their assets. It is important to maintain two-way information exchange because one-way flow is unlikely to be sustainable in the long term. Without seeing clear interest from government, critical infrastructure operators are usually reluctant to cooperate even if legally obligated.

As countries gain more experience in CIIP, it becomes more evident that the public sector cannot secure all critical infrastructure assets at all times. Operators of critical infrastructures cannot expect NCIPAs to protect and secure assets because they do not own the infrastructure. Even if that was possible, it would require substantial financial and human resources. Therefore, CIIP policies must focus on supporting and advising critical infrastructure operators in their efforts to protect assets as an alternative to substituting those efforts. This approach is considered more sustainable in the long term because it eventually increases the capacity of critical infrastructure operators and the resilience of their assets. Information sharing is an example of this policy approach. While increasing its capacity to monitor and provide early warning at the national level, the public sector could play an important role in sharing this information with all critical infrastructure operators. As a result, each critical infrastructure operator is individually empowered to take preventive and/or defensive measures.[1] This way, the public sector invests in systems that benefit overall CIIP objectives, extending the reach of CIIP activities and enabling the efforts of each party to complement each other.

There are more instances of the public sector providing valuable input into the CIIP implementation process without input from the private sector. Spain is one example. The National Center for the Protection of Critical Infrastructure (CNPIC), Spain's NCIPA, is in charge of technically implementing the CIIP framework. For example, it promotes, coordinates, and supervises all CIP-related activities at the national level. The CNPIC's main objective is to promote and coordinate the mechanisms needed to guarantee the security of the infrastructures that supply services essential to society. The CNPIC oversees the National Strategic Infrastructure Catalogue and has set up a Security Incident Response Team specialized in analyzing and managing problems and incidents related to technological security. If a critical infrastructure is affected by a cyber-security incident, the operator responsible for it is able to use the services provided by the Response Team.

The Centre for the Protection of National Infrastructure (CPNI), the UK's national NCIPA, provides advisory services such as information,

[1] Prevention aims to decrease the risk related to critical infrastructure security and functionality. Defensive measures are steps taken to detect attacks and incidents and react to them or limit their negative impact.

personnel, and physical security guidance to the businesses and organizations that manage the nation's critical infrastructures. These activities aim to reduce vulnerability to terrorism and other threats. As needed, the CPNI can call on resources from other government departments and agencies, including their domestic counter-intelligence and security agency, Military Intelligence Section 5, the Communications-Electronics Security Group, and other government departments responsible for national infrastructure sectors.

In Finland, the role of NCIPA is performed by the National Emergency Supply Agency (NESA). NESA has a role in securing critical infrastructures by developing and financing both technical backup systems and electromagnetic pulse secure premises for systems. Finland's vital information and communications technology (ICT) systems are located in the capital region and this concentration in one area poses a risk. Therefore, NESA owns two computer backup co-location centers outside the capital region to secure the nation's critical information technology (IT) systems.

In South Korea, the supervision of CIIP is performed by its multi-institutional, hierarchical structure chaired by the Prime Minister and comprising vice minister-level officials of related central administrative agencies. This structure oversees the designation of critical infrastructures, and coordinates and deliberates on protection policy and plans. The MSIP and the NIS form the Working-Level Committee and authorize guidelines to design relevant plans to confirm the adequacy of protective measures. The NIS Director and the Minister of the MSIP also inform the head of the relevant central administrative agency of the confirmation results regarding implementation of protective measures.

Private Sector Approaches

In most countries, the responsibility for the resilience of critical infrastructures lies with the owners and operators. This is one of the guiding principles of many CIIP frameworks. The responsibility encompasses a number of activities that critical infrastructure operators are expected to carry out. One such activity is to identify (or participate in identifying) the critical assets and then ensure the resilience of those assets. More specifically, critical infrastructure operators are asked to identify and classify the infrastructures supporting critical applications, according to their criticality. They are responsible for determining the core processes and the respective applications and services (solutions) that are used to operate the applications.

Critical infrastructure operators are susceptible to risks that may have a detrimental effect on society. These risks may be directly linked to the critical service provided or may emerge from activities that are not related to the core business of the critical infrastructure operator. Operators of critical infrastructure are in charge of operating and securing their infrastructures, and thus could also be legally obliged to carry out risk assessment analysis and submit business continuity plans to the responsible government authorities. In some critical infrastructure sectors, they are also obliged to comply with certain regulations that could impact the operation, infrastructure, and/or data networks. An example of such a sector could be finance (ENISA, 2015). To comply with regulations, operators of critical infrastructure classify their infrastructures and processes as well as the respective supporting applications and information. This is led by prioritizing the critical infrastructure and adopting requirements for high priority infrastructures. In certain cases, operators of critical infrastructure have a highly diversified portfolio of services and respective infrastructures. Such operators need to apply a diversified approach according to service criticality.

Currently there is no legal obligation for critical infrastructure operators to classify their own infrastructure assets in Finland, the UK, or Spain. However, the designated critical infrastructure operator is required to identify their relevant assets and services as critical from the perspective of operators. Afterward, the authorized government institutions classify information by the criteria of national dependency on infrastructures and compose national critical infrastructure lists. Critical infrastructure operators are responsible for preparing security and contingency plans to increase the resilience of their own critical infrastructure assets.

Sharing information related to different aspects of the critical infrastructure is a common responsibility of the operators. Given that information exchange is kept confidential, operators are invited (less frequently obliged) to provide a pre-defined list of information, including relevant real-time information on the state of operated critical infrastructures. In the United States, operators are invited to share relevant information through the Protected Critical Infrastructure Information Program on a voluntary basis. A similar initiative is in place in the UK.

It is also common for critical infrastructure operators, from the same or different sectors, to organize a forum to collaborate, share information, build capacity, and exchange expertise. One example of such an initiative is the Association for the Protection of Critical Infrastructure, which was established in Spain in 2011.[2] The association is a non-profit legal entity that serves as a forum for debates about sectoral threats and risks, bringing together professionals and experts to strengthen the capacity of its members. It also functions as a liaison for security professionals in matters of civil information, security, fire safety, and environmental protection.

There are also examples of industry-organized bodies that work to improve CIP at the sectoral level. For instance, the Finnish Information Security Cluster,[3] created in 2012, is an association authorized by major Finnish information security companies to promote their business and operations in national and international contexts. It is very active in business advocacy and is significantly engaged with important national projects. One such project is Situation Awareness in Informatics and Cyber Security, a national research project funded by Tekes (the Finnish Funding Agency for Innovation) and the Academy of Finland to improve critical infrastructure with critical stakeholders domestically (academic institutions such as Aalto University, University of Jyväskylä, and University of Oulu) and abroad.

Public–Private Partnerships

The industry's perception of government's capability to manage critical situations is very important for building trust and cooperation. It is particularly important (and challenging) for governments to maintain high capacity and organizational readiness that allows industry to feel it is an equal partner. Indeed, countries demonstrating highly evolved public–private cooperation in CIIP are also those countries where industry perceives that their governments are mostly or fully capable of adequately managing critical situations. For instance, in 2010, regarding cyber-attacks on critical infrastructure, over 60 percent of industry representatives in the UK and the United States regarded their governments as being mostly or highly capable of preventing or deterring a cyber-attack (Baker, Filipiak, and Timlin, 2011). Both countries have well regarded public–private cooperation frameworks and practices. At the same time, over 80 percent of industry representatives surveyed in Brazil said they had no confidence in their government's abilities to prevent or deter a cyber-attack, and in Mexico the number was approximately 70 percent.[4] In these countries, public–private cooperation is weaker.

The mechanism to advance collective action toward national critical infrastructure security and resilience in the United States is based on voluntary collaboration between critical infrastructure owners and operators (including their partner associations, vendors, and others) and their government counterparts. Since 1998, the first Presidential Directive on CIP encompassed separate articles dedicated to public–private cooperation (see *CIIP Policy and*

[2] Asociación para la Protección de las Infraestructuras Críticas, at: http://infraestructurascriticas.com/principal.asp?pag=.

[3] www.fisc.fi.

[4] Ibid.

Governance in the United States in Chapter 2). The approach for PPP was to work within the set of areas through the designated Sector Liaison Officer on the public sector side and Sector Coordinator on the operator side. The areas identified for cooperation included assessing the sector's vulnerabilities to cyber or physical attacks and making recommendations to eliminate significant vulnerabilities. Together, these individuals were expected to contribute to a sectoral National Infrastructure Assurance Plan.

Similar approaches of building a network of representatives and organizing relevant activities was adopted in many other countries. This approach laid the groundwork for joint collaboration, including determining CIIP-related initiatives and increasing the resilience and security of national critical infrastructures. The experiences of the countries studied for this report suggest that it is the NCIPA that most commonly represents the public side in CIIP PPP initiatives. Indeed, in Spain, the CNPIC represents the public side within the CIIP PPP initiatives, the Department of Homeland Security in the United States, CPNI in the UK, NESA in Finland, and the European Agency for Network and Information Security in the EU.

In the United States, the Department of Homeland Security is performing the NCIPA function. In 2006, the Secretary of Homeland Security instituted the Critical Infrastructure Partnership Advisory Council. This touchstone provided the legal framework for a cross-sector partnership mechanism to directly support various sectors' interests in engaging in public–private critical infrastructure discussions and participating in a broad spectrum of activities.[5] Specifically, the forums held by this council support federal government deliberations on critical infrastructure issues needing a consensus when making formal recommendations. Sector and cross-sector coordinating structures are defined in the National Infrastructure Protection Plan.

The UK's CPNI, its national NCIPA, maintains close relationships with organizations and firms that own and/or operate national critical infrastructures. Relationships have been cultivated over many years between experienced security advisers and managers. CPNI provides guidance in a variety of ways, through face-to-face consultations by teams of specialists, training, online advice, and written reports.

The CPNI facilitates information sharing of CIIP research among stakeholders to inform them of successful security planning across sectors. It also disseminates information related to a wide range of physical security products developed by manufacturers of security equipment for use within critical infrastructure sites. Furthermore, the CPNI works with external partners to set professional standards, maintaining the Register of Security Engineers and Specialists. This register was created to promote excellence in the field of security engineering and provide a means for individuals to demonstrate competence in this discipline through independent assessment. It is sponsored by CPNI and is administered and operated by the Institution of Civil Engineers.

In Finland, the NESA,[6] which ensures the security of supply for strategic services for society, collaborates with other organizations within the National Emergency Supply Organization (NESO).[7] NESO facilitates cooperation between the public and private sectors by creating a vehicle for PPP initiatives (Box 4.1).

At the level of critical infrastructure sectors, there is also a need to involve sectoral organizations such as regulatory agencies. Some CIIP PPP activities are led or co-led by such agencies. For instance, in Finland, the Finnish Communications Regulatory Authority is very active in CIIP, as is the Korea Internet and Security Agency.

In the UK, the sectoral level PPP is implemented through thematic working groups, for instance the Electronic Communications Resilience and Response Group (UK, 2013a). This group leads in developing and maintaining cooperation between the telecommunication industry and government by:

[5] CI Partnership Advisory Council homepage: http://www.dhs.gov/cipac-sector-charters-and-membership.

[6] http://www.nesa.fi/security-of-supply/.

[7] http://www.nesa.fi/organisation/.

Box 4.1. National Emergency Supply Organization

The NESO is a network that maintains and develops the security of critical supply of services in Finland on the basis of PPP initiatives. Its primary objective is to ensure the conditions necessary for the operations of organizations that are critical to security of supply. Hundreds of enterprises, government authorities, and associations from various sectors of society are active in pursuit of NESO's shared mission.

The NESO consists of the National Emergency Supply Agency (NESA), the National Emergency Supply Council, and the individual NESO sectors and pools.

The **NESA** is tasked with planning and measures related to developing and maintaining security of supply. The statutory duties of the agency include providing support for the operations of the pools and sectors. It is led by a chief executive officer in accordance with guidelines issued by the NESA Board of Directors.

The **National Emergency Supply Council** is a body that assesses and reviews the general state of security of the supply chain.

The general mandate for the **NESO sectors** is to steer, coordinate, and monitor preparedness in their respective fields and to determine the goals for the pools.

The business-driven **NESO pools** are responsible for operational preparedness in their fields. The pools are tasked with monitoring, analyzing, planning, and preparing measures to develop security of supply within their individual industries, and with determining which enterprises are critical to security of supply.

Source: http://www.nesa.fi/organisation/.

- Providing a forum to exchange information between industry experts in telecommunications and government with policy interests in resilience;
- Planning, including ownership of the National Emergency Plan for the telecommunications sector; and
- Providing response capability for emergencies through the National Emergency Alert for Telecommunications.

The group is chaired by an industry representative and hosted by the Department for Business, Innovation and Skills, and meets four times a year. Similar groups exist in other critical infrastructure sectors. For example, in the downstream oil and gas subsectors of the energy sector, governmental responsibility for CIIP is assigned to the Department of Energy and Climate Change. For the purpose of PPP, the department's coordination group (UK, 2103c) was formed to play the key role in fostering joint industrial and governmental work that responds to disruptions (or potential disruptions) to the energy supply chain. The coordination group acts through the same vital areas as telecommunications:

- Exchanging information between industry and respective governmental authorities;
- Planning the crisis management system through, for example, public consultations and annual exercises, and coordinating individual corporate emergency plans using the crisis management system; and
- Providing capabilities to respond to emergencies through:
  - Initial evaluation, by exchanging information between operators and governmental officials and initiating further steps for crisis management procedures; and
  - Implementing the Department of Energy and Climate Change Upstream Crisis Management Plan by assessing the information received and providing consolidated advice about CIIP to the sector on the emerging situation.

Similarly, in the United States, under the framework of the Critical Infrastructure Advisory Council, there exists the Sectoral Coordinating Councils. Each council comprises government and sector charters. Each charter operates under unique articles.

Box 4.2. Information Exchange for Critical Energy Infrastructure Protection in the EU

As a result of the adoption of the CIP Directive, the European Commission created the Thematic Network on Critical Energy Infrastructure Protection (TNCEIP). This initiative is hosted within the Directorate General Energy. The TNCEIP comprises owners and operators of European energy infrastructure in the electricity, gas, and oil subsectors. This thematic network allows operators to exchange information on threat assessment, risk management, cyber security, etcetera.

The TNCEIP organizes periodic meetings that are hosted by different member states across the EU. This facilitates exchange of practices on infrastructure protection issues and closer collaboration among the energy operators and institutions from different countries. In 2013, TNCEIP meetings were hosted in Ispra, Italy, and Vienna, Austria. The meeting in Italy was dedicated to interdependencies, including interdependency between energy and ICT. In Austria, the meeting was dedicated to issues of physical security in the energy sector, such as Physical Protection Systems. In 2014, the TNCEIP meeting, which was hosted in Madrid, Spain, was dedicated to experiences in international collaboration, exchange of best practices, transfer of knowledge in security (both physical and cyber) between subsidiaries in different countries, and coordination for resolving international crises.

The TNCEIP is launching a periodical newsletter, representing the position of energy operators and owners regarding policy and legislative processes at the EU level. In 2012, during the review process of the EPCIP and CIP Directive, the TNCEIP issued a Position Paper, *EU Policy on Critical Energy Infrastructure Protection* outlining the position of the EU energy sectors on the priorities that new programs should embrace.

Source: Authors based on DG ENER, http://ec.europa.eu/energy/, TCNEIP Newsletter, EC (2012b).

For instance, the Communications Coordination Council exists under the Communications Sector Coordinating Charter[8] and Communications Government Coordinating Charter.[9] Sector coordinating charters are self-organized and comprise critical infrastructure operators and owners, while government coordinating charters comprise public sector institutions, including sectoral agencies.

A similar approach is observed in the EU. For instance, in the energy sector, the European Commission supported the inauguration of the Thematic Network on Critical Energy Infrastructure Protection (TNCEIP) (Box 4.2).[10] This network brings together critical infrastructure operators, representatives of member states, and the European Commission and serves as a forum for information exchange and cooperation.

Partnering at the sectoral level usually involves more stakeholders. Spain's Cyber Security Institute promotes knowledge sharing and collaboration among the main actors and experts involved in the sector to improve cyber security in the country.[11] The institute carries out analytical work (studies), awareness (events), and training (certification in cyber security), among others. The UK funded the Global Cyber Security Capacity Centre[12] as part of Oxford University's Martin School.[13] The center is a global thought leader in cyber security that implements the best practice working archetype of governments working with academia and industry to create the best policy. Among many of its initiatives, the center has developed the Capacity Maturity Model, designed to identify needs for capacity

[8] Article of operation of Communications Sector Coordinating Charter at: http://www.dhs.gov/cipac-sector-charters-and-membership.

[9] Article of operation of Communications Government Coordination Charter at: http://www.dhs.gov/sites/default/files/publications/cipac-comms-gcc-charter-508.pdf.

[10] http://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure.

[11] https://cybersecuritymonth.eu/ecsm-countries/spain/iii-cyber-security-forum-of-the-spanish-cyber-security-institute-an-isms-forum-iniciative.

[12] Under the National Cyber Security Program, see *CIIP Policy and Governance in the UK* in Chapter 2.

[13] http://www.oxfordmartin.ox.ac.uk/research/programmes/cybersecurity/.

Box 4.3. **Cyber Security Capacity Maturity Model**

The Global Cyber Security Capacity Centre promotes an increase in the scale, pace, quality, and impact of cyber security capacity-building initiatives around the world. Among its initiatives, the center has created a first-of-its-kind benchmark to measure cyber security capacity maturity across five dimensions. The aim of the benchmark is to help nations self-assess, benchmark, plan investments and national cyber security strategies, and set priorities for capacity development.

Working with key stakeholders from across the international community, the center has begun to successfully apply the model globally, alongside partners such as the World Bank, Organization of American States, and Commonwealth Telecommunications Organization. The first report released as a result of this work was launched in June 2015 in Kosovo.

Source: Based on Global Cyber Security Capacity Centre, http://www.oxfordmartin.ox.ac.uk/cybersecurity/; Cyber Center works with the World Bank in Kosovo, 2015, http://www.oxfordmartin.ox.ac.uk/news/2015-GCSCC-Kosovo-launch.

building, and has developed global security capacity (Box 4.3). A new web portal facilitates greater information exchange among researchers and consumers of research in cyber security, and acts as a resource for experts and international partners.[14]

The Korean government organized information sharing and analysis centers to provide technological support through their CIIP Law (see *CIIP Policy and Governance in Korea* in Chapter 2). These centers serve to protect CII by sector, such as finance and communications. They may provide information about vulnerabilities, intrusions, and countermeasures, and they may operate real-time alarm and analysis systems if incidents occur.

Furthermore, PPPs related to CIIP are increasingly going beyond the private and public sector stakeholders, with the general public increasingly being involved. For instance, as part of its CIIP effort, the United States is building a nationwide awareness campaign about critical infrastructure, its importance, and the need to protect it. For example, November is now the month to recognize National Critical Infrastructure Security and Resilience (Box 4.4).

Observations and Recommendations Regarding Critical Infrastructure Protection

Complementarity of efforts between the public and private sectors: CIIP policies should focus objectives and activities on supporting critical infrastructure operators in their efforts to protect operated assets as an alternative to substituting those efforts. This approach is considered to be more sustainable in the long term as it eventually allows for increased capacity of operators and resilience of critical infrastructure assets. It also expands the reach of CIIP activities and complements the efforts of each party.

Partnering with the private sector: It takes time and effort to build the level of trust and cooperation needed for CIIP. It took 10 to 15 years for countries to put in place successful partnerships and deepen the level of cooperation. It will take time for developing countries to build effective partnerships because they require comparable capacity and capability from both sides. The public sector must be perceived as a strong partner in CIIP. Leveraging national and regional academia for targeted research and development in CIIP may be a good way forward in increasing the capacity of the public sector in decision-making, providing expertise and advice to the private sector.

Partnering structures: This study showed that it is efficient to introduce contact points within critical infrastructure sectors and the public sector. It is

[14] www.sbs.ox.ac.uk/cybersecurity-capacity.

advisable to maintain a sectoral approach for CIIP cooperation as it allows for specific discussions of sectoral aspects of CIIP implementation and measurement. Successful cases of cooperation demonstrate that it is possible to engage private sector actors in the administration of sectoral structures, such as co-leadership, organization of meetings, and election of topics.

Establish sectoral CIIP working groups and develop a CIP community: For all critical infrastructure sectors, but particularly for those sectors with high participation of the private capital and large number of actors (e.g., ICT, transport, and financial), it is advisable to commission CIIP-dedicated working groups or committees that would be led or co-led by the private sector. Those bodies would be instrumental in preparing and implementing the national and sectoral CIP plans, enhancing information exchange, and building the CIP community. Regular CIP events at the national level as well as regular sectoral gatherings to discuss current issues promote the CIIP agenda and identify where efforts should be strengthened. Through these structures, international cooperation, and exchange of professional experience in CIIP would be accomplished.

Involve academia and the research community: Assessments of the vulnerabilities and risks as well as other highly analytical work require considerable research capacity that is usually not available within public institutions. Quality CIIP plans cannot be built without such scientific foundation. As a result, countries examined in this chapter outsourced that capacity to national institutes and research centers. Latin American and Caribbean countries and the region should also consider this approach. There could also be an opportunity to build collaboration between academia and the public sector, where national standardization agencies could also participate.

5

Information Sharing and Incident Management for CIIP

Who Shares What and When?

Information sharing is the most important element of each stage of the critical information infrastructure protection (CIIP) process. It provides better understanding of threats, risks, and dependencies, expediting knowledge sharing of possible countermeasures. Bi-directional information sharing is recommended, meaning both public and private sectors need to be involved and information needs to circulate in both directions. Thus, information sharing is a public–private partnership (PPP)-type of activity. At the same time, information sharing within the public and private sectors is important. In the private sector, knowledge exchange is important not only within the same critical infrastructure sector, but also between the different sectors because of the high convergence. For instance, the financial sector may benefit from input from the information and communications technology (ICT) sector because of the financial system's depen-dency on electronic communications.

A common operational landscape for information sharing is presented in Table 5.1. It is best for governments and industry to work together to designate *who* shares *what* and *when*. The table offers some best practices from the United States on how tasks could be divided among the public and private sectors, as well as what agencies could be involved.

In particular, efficient dissemination of information is essential for CIIP because of the interconnectedness of assets nationally and internationally. For critical information infrastructure (CII), Spain uses the System for the Exchange of Information and Reporting of Incidents to coordinate, cooperate, and exchange information that affects national interests with the central government, autonomous

TABLE 5.1. Information Sharing in the United States: Key Dimensions

What to share	Who should share	When to share	How to protect shared information
Government: Threat intelligence Warnings and advisories **Private sector:** Vulnerabilities Solutions Advisories	Intelligence agencies Law enforcement agencies Critical infrastructure owners/ operators Coordination partnerships (at all levels)	**Pre-event:** Advisories Warnings **During and after the event:** Remediation steps Coordination of resources	Public key infrastructure Strong policies, with penalties for misuse

Source: Authors based on U.S. practice.

Box 5.1. Benefits of Information Sharing to CIIP

Information sharing has the following benefits for CIIP:

- Raises awareness of the need to perform CIIP and related topics such as business continuity management and risk management.
- Improves the level of education and knowledge about the subject.
- While sharing experience, increases the skills of community members.
- While following the topics discussed within the communities, serves as a channel to keep the government involved in the concerns of the community.
- While using the private community, the government can directly address all or part of the community with specific information. If the community uses a secure communication channel, this can even include restricted information.

Source: EC (2011).

regions, local authorities, the private sector, EU institutions, other member states, and relevant international bodies to ensure awareness, capacity building, and response competency.

How to Share?

It is common to hear that public and private stakeholders are largely unaware of critical infrastructure protection (CIP) and therefore that awareness should be increased. But what does it mean to increase CIP awareness? What actions can lead to it?

To begin, both parties (governments and critical infrastructure operators) need to have a good understanding of each other's roles as well as some underlying concepts and information. For example, public sector stakeholders should be familiar with critical infrastructures, entities that manage them, and cross-sector interrelations (impacts) and risks. In turn, critical infrastructure operators should have a clear understanding about the public sector approach to CIIP, the distribution of functions and responsibilities across different public agencies, and their own role and responsibilities within the national CIP framework.

This process improves the quality of risk management across participants, and may thus raise the level of protection. On this basis, CIP policymakers will have a better understanding of the level of protection and possible contingencies. For example, sharing security information creates preconditions for an effective incident prevention system. Such common understanding will prove to be essential in the case of a major incident where crisis management is required (Box 5.1).

To support the CIIP process, sharing could cover information about threats and vulnerabilities, good practices for technical and organizational protection measures, or security incidents in critical infrastructure data. It is important to have this exchange in a trusted and secure manner as the nature of this information is usually sensitive. To guarantee the confidentiality of the information exchange, the most widely used tool is the Traffic Light Protocol (TLP), considered to be one of the best practices (EC, 2011). TLP provides an easy method to achieve confidentiality of sensitive material. One of the key principles of TLP is that the originator of the sensitive information also decides how widely it can be circulated by labeling the information with one of four colors (Table 5.2).

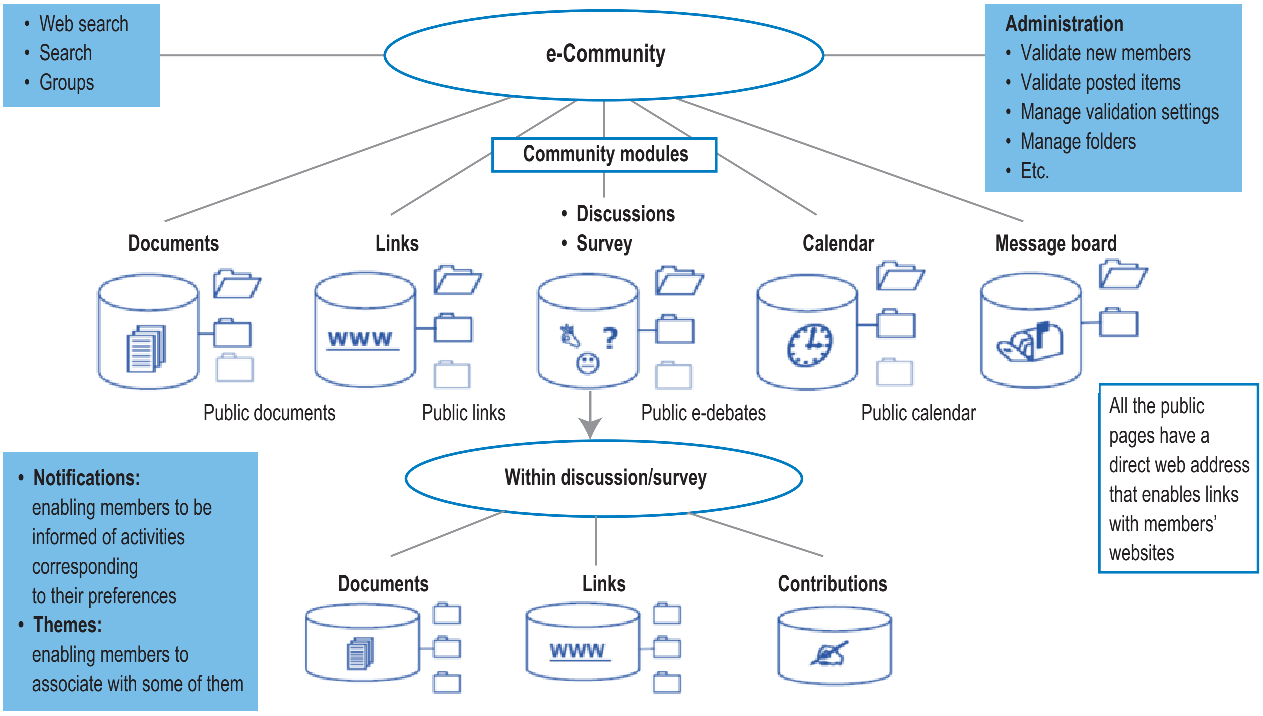
The originator needs to ensure that the information provided corresponds to the code description and that the recipients are alerted about the new threat and are able to take appropriate actions. Above all, the information provider remains the owner of the shared information and its sensitivity classification.

TABLE 5.2. TLP Color Code

Color	Meaning
Red	Personal for named recipients only. In the context of a meeting, for example, RED information is limited to those present at the meeting. In most circumstances, RED information will only be passed verbally or in person.
Amber	Limited distribution. The recipient may share AMBER information with others within their organization, but only on a need-to-know basis. The originator may be expected to specify the intended limits of that sharing.
Green	Community wide. Information in this category can be circulated widely within a particular community. However, the information may not be published or posted publicly on the internet, nor released outside of the community.
White	Unlimited. Subject to standard copyright rules, WHITE information may be distributed freely, without restriction.

Source: EC (2011).

FIGURE 5.1. Critical Infrastructure Warning Information Network Scheme



Source: European Commission.

Most sharing initiatives are based on regular face-to-face meetings. If the report on vulnerabilities, threats, and incidents has to be shared with a wider community, a secure electronic environment proves to be useful. One example of an exchange platform was developed in the EU, the Critical Infrastructure Warning Information Network.[1] The network is an initiative of the European Commission that is being coordinated by its Directorate General for Home Affairs (Figure 5.1). Since its initiation in 2013, the network's objective has been to improve CIP in Europe by exchanging and discussing CIP-related information, studies, and good practices across all of the EU member states and in all relevant sectors of economic activity.

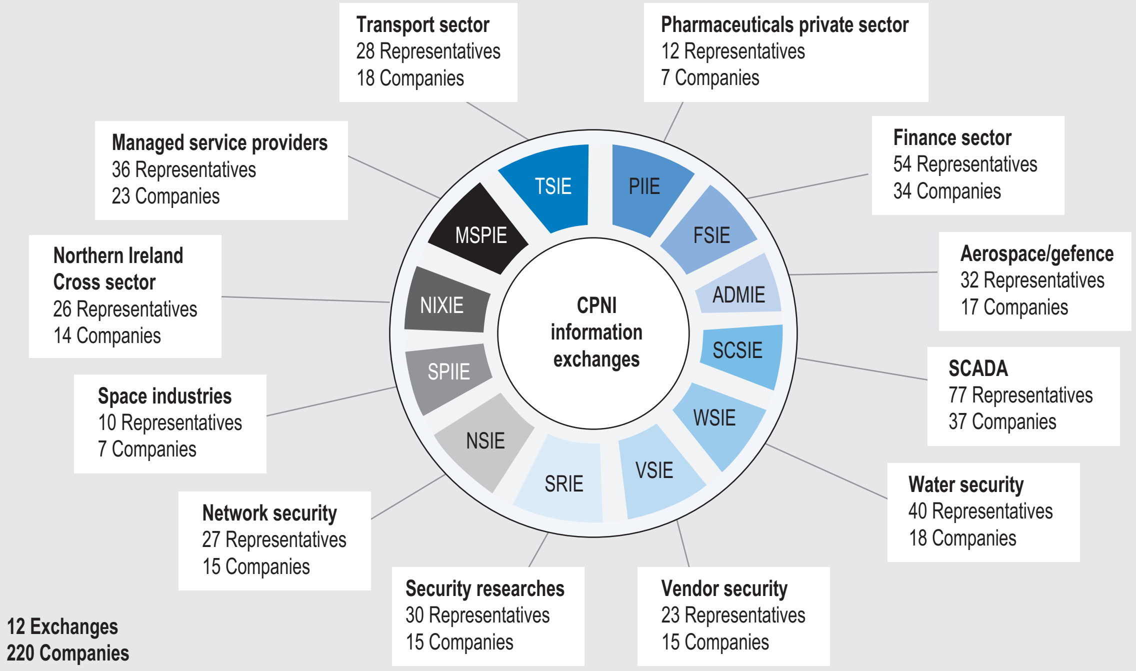
[1] http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm.

Box 5.2. UK Cyber-Security Information Sharing Partnership

The Cyber-Security Information Sharing Partnership was funded under the UK's National Cyber Security Program as part of the Cyber Security Strategy. Information is exchanged in relation to cyber-attacks and vulnerabilities to physical and personnel-related threats.

Information exchanges bring together representatives from a specific critical infrastructure or across multiple critical infrastructures. They also include relevant public organizations like law enforcement or intelligence services. Information exchanges are free to join and their membership is determined by the existing members. CPNI typically provides a co-chair and a coordinator for the exchange and acts as host for the meetings. Representatives at information exchanges are expected to attend all meetings and generally only two named members from the same organization are allowed. Substitutes cannot attend. Information exchanges include elements presented in Figure 5.2.

FIGURE 5.2. CPNI Model of Information Exchange



Source: CPNI.

To further good practices, some countries have formed small trusted communities in which information can be shared in a secure and trusted way. For instance, the UK's Centre for the Protection of National Infrastructure (CPNI) launched the Cyber-Security Information Sharing Partnership program in 2012. This program is a joint initiative between industry and government. The goal is to share cyber threat and vulnerability information to increase overall situational awareness, reducing the negative impact on domestic businesses (Box 5.2) (UK, 2013b).

Protecting confidentiality is an important subject for information providers, in particular those in commercial critical infrastructure sectors. Information that is valuable for CIP may be commercially sensitive and its disclosure may have a dramatic effect. Thus the sharing process should follow (whenever

Box 5.3. United States Protected Critical Infrastructure Information Program

In 2002, the United States adopted a Protected Critical Infrastructure Information Program. The program aims to strengthen CIP-related information exchange. It provides legal certainty regarding how and by whom information can be received and used. Specifically, the legal requirement is such that protected critical infrastructure information cannot:

- Be disclosed through a *Freedom of Information Act* request or through a request under a similar state, local, tribal, or territorial disclosure law;
- Be disclosed in civil litigation; or
- Be used for regulatory purposes.

Protected information can only be used by a federal, state, local, tribal, or territorial government employee or contractor who:

- Has taken appropriate training;
- Has homeland security duties; and
- Has a valid need to know that particular information.

Protected critical infrastructure information is specially marked and must be safeguarded, both physically and electronically, under specific procedures to avoid any improper disclosures. All of these protections ensure that submitted information is protected and is used only by authorized homeland security professionals and used only for homeland security purposes.

Source: DHS (2014).

possible) a voluntary approach, with aspects of confidentiality (regulated disclosure) explicitly mandated within the relevant legal regulatory framework. Such is the case in the United States, where separate legislation dedicated entirely to CIP information sharing (Box 5.3) needs to be adopted.

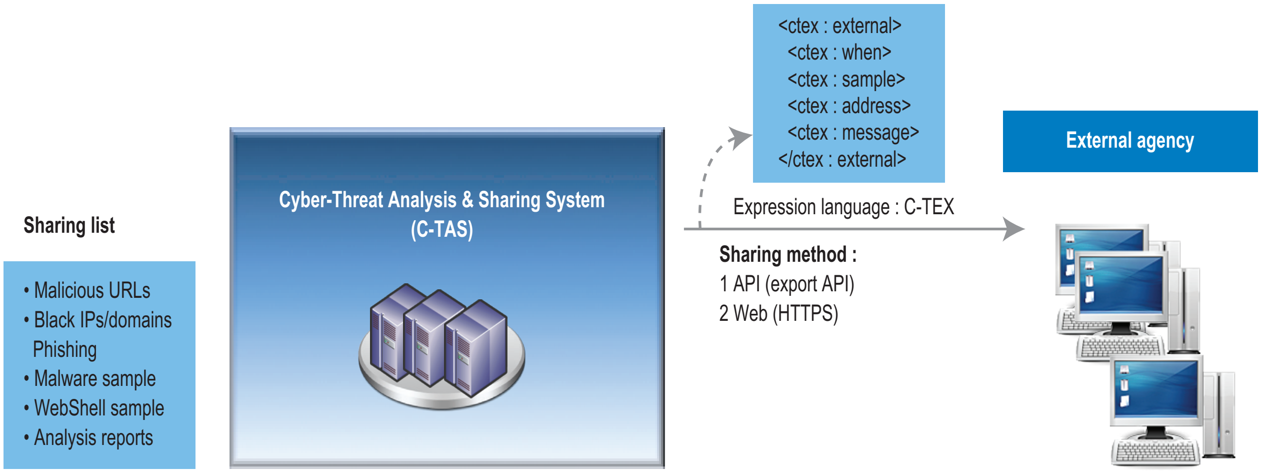
In Korea, the Cyber-Threat Analysis and Sharing System was developed to systemize the procedures of intrusion detection, collection, analysis, and cyber-threat data exchange and to prompt countermeasures. The system collects various data from many enterprises, including security companies, popular web sites, and Korea's in-house computer emergency response team's system. It provides 36 types of reports for security vulnerabilities, fraudulent domains, and technical reports, among others, based on collected and analyzed data. The information is shared with external agencies through an Application Program Interface (API) and homepage (Figure 5.3).

Cross-Border Information Sharing

Information sharing and analysis is paramount in understanding cross-border interdependencies; however, installing sharing practices is particularly challenging. Cross-border information exchange on a bilateral basis is instituted in nearly all case study countries examined in the previous sections of this book. The authors have observed that information exchange at the multi-national and regional level proves to be very valuable as it provides a strong networking opportunity and reinforces bilateral relationships. Hence, the authors recommend information exchange in developing countries to join the international CIP community and start collaborating.

However, initiatives that bring the CIP community together are limited and few are dedicated specifically to shaping information exchange on a multilateral level. One of the largest international

FIGURE 5.3. Information Sharing for PPP



Source: http://www.krcert.or.kr/.

information sharing initiatives currently in place is known as the Meridian Process. This initiative's ambitious objective is to exchange ideas and initiate actions for the cooperation of governmental bodies on global CIIP issues through a community of CIIP senior government policymakers and provides a forum to share international best practices. The Meridian Process is guided by the principle that advances in national CIIP goals are only possible through close collaboration beyond national borders and even beyond regions. Participation in the initiative is open to all nations (Box 5.4).

The Meridian Process produces the CIIP Directory, an authoritative compilation of CIIP points of contact around the world, and particularly within the Meridian Community. The CIIP Directory is disseminated using TLP and only available to community members. The directory is intended for national governments only. It is not intended for general or commercial use. Each country nominates a Directory Point of Contact who maintains and updates their country's entry details.

In the context of cyber security, another international initiative is the Global Forum for Incident

Box 5.4. Meridian Process

The Meridian Process emerged from the first Meridian Conference, hosted by the UK in 2005. The host country changes each year with the aim to increase participation in the Meridian Community. Any country that is engaged in CIIP and has attended more than one event can offer to host a forthcoming event. The host country is usually decided two years in advance through discussion with the Steering Committee and an endorsement from fellow delegates.

Each annual conference has been followed by an initiative in CIIP taken up by the host country to strengthen the process, and various cooperative activities among members of the Meridian Community. Every country that sends a delegate to a conference automatically becomes a member of the community and is entitled to an entry in the Meridian Directory and access to its resources and activities.

Source: Authors based on The Meridian Process official web-site, http://www.meridianprocess.org/.

Box 5.5. Establishment of the Global Forum for Incident Response and Security Teams

In November 1988, a computer security incident known as the "internet worm" brought major portions of the internet to its knees. Reaction to this incident was isolated and uncoordinated, resulting in duplicated efforts, and in conflicting solutions. Weeks later, the Computer Emergency Response Team's Coordination Center was formed. Soon after, the U.S. Department of Energy formed the Computer Incident Advisory Capability to serve its constituents.

Over the next two years, the number of CSIRTs continued to grow, each with its own purpose, funding, reporting requirements, and constituency. The interaction between these teams was challenging because of the differences in languages, time zones, and international standards or conventions. In October 1989, a major incident called the "wank worm" highlighted the need for better communication and coordination between teams.

The Global Forum for Incident Response and Security Teams was formed in 1990 in response to this problem. Since then, it has continued to grow and evolve in response to the changing needs of the incident response and security teams and their constituencies.

Source: Global Forum for Incident Response and Security Teams, at: https://www.first.org/about/history.

Response and Security Teams. This forum comprises 330 accredited members and is the only organization enabling cooperation among computer security incident response teams (CSIRTs) on a global scale. The forum brings together a variety of CSIRTs from government, commercial, and educational organizations. It aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. The forum also aims to standardize information sharing practices across its members and beyond. For instance, one of its special interest groups is working toward preparation of "*a common, standardized set of definitions for all Traffic Light Protocol colors in English, a clear usage guide explaining how, when, and where TLP should be used to be most effective, and a governance document to explain the rules by which the [special interest group] will govern the TLP standard in the future.*" The group plans to present its initial results in June 2016.[2]

Crisis Management Practices

The security paradigm states that absolute protection status is not possible, even in hypothetical situations when all measures are perfectly implemented. Incidents are inevitable since threats will materialize. Parties involved in CIIP should thus be prepared for crisis situations and plan defense actions. The Latin American and Caribbean region includes nine of the world's top 20 disaster prone countries (World Bank, 2016). Mitigating, preventing, and dealing with natural disasters cost these governments about $2 billion a year (World Bank, 2016).

The term crisis is defined as a major incident where a supervisory organization and/or critical infrastructure operator loses its ability to manage and control the escalating situation. Crisis management is the process by which an organization deals with a major event that threatens to harm the organization, its stakeholders, or the general public. The government's role is to ensure that crisis management agencies are organized, understand their roles, and have resources to deal with incidents and emergencies to mitigate dramatic consequences for the public.

The continuity of critical infrastructure services to perform crisis management functions is often critical to counter operations, which consist of

[2] See https://www.first.org/global/sigs/tlp.

the preparedness, response, and recovery phases. Crisis management includes the ability to operate national and regional crisis control center(s) and local centers that support incident response actions in the field. It is important to note, that critical infrastructure operators are responsible for using measures to avoid disruptions and having a plan for rapid service restoration. Whoever is responsible for situation management is also responsible for communications.

Effective and efficient crisis management requires in-depth knowledge of critical infrastructures, their operations, and their dependencies. Close cooperation and mutual understanding with operators is required during incident response planning, emergency preparedness (e.g., joint training and exercises), crisis response, and restoration. Some countries legally oblige critical infrastructure operators to form a critical infrastructure sector-specific crisis management arrangement or formally be a part of the national or regional crisis management structure. Dedicated laws may thus be required to actively involve critical infrastructure operators in the preparedness, countermeasures, and service restoration phases of crisis management. Moreover, legislation for crisis management can be sector-specific or can cover all critical infrastructure sectors.

Sector-specific legislation is made either by the ministry responsible for the sector or by the relevant regulatory agency, with possible input from stakeholders. Broad legislation can be a framework within which critical infrastructure operators are mandated to collaborate with regional crisis management entities. It may also provide a framework for crisis management at the national level. For example, the UK approach is based on section 32 article (4) (a) and (b) of the *Communications Act* 2003 in relation to the *Civil Contingencies Act*. The Electronic Communication Resilience and Response Group comprises operators forming the national response capability for ICT emergencies through National Emergency Alert for Telecommunications.[3] In Finland, the Cabinet Committee on Foreign and Security Policy acts as the contact point for stand-by duties of the ministries. It keeps the administrative sectors informed about observed events and, when necessary, convenes the cooperation bodies and experts from different administrative sectors to secure up-to-date access to information (Finland, 2011). Other critical infrastructure sectors, such as the financial sector, have formed similar business continuity and crisis mitigation plans.

An adequate level of preparedness to manage crisis situations could be achieved through simulation exercises at the operational, tactical, and strategic levels and/or spanning multiple levels. Exercises increase the level of readiness for emergencies and enhance the operators understanding of their roles, responsibilities, decision-making cycles, and capabilities.

Incidents Management via CSIRT

The quantity and sophistication of cyber security incidents increased dramatically in recent years and both continue to intensify. Cyber-attacks have an impact not only on the ICT sector but are also significant threats to almost all critical infrastructures, such as Supervisory Control and Data Acquisition Systems.

CSIRTs respond to network and information security incidents. Their main role is to quickly address security incidents in electronic communications networks, and analyze and coordinate actions to contain and eliminate threats, especially when there is a potential risk to functionality of the network or security of the data. CSIRTs could be regarded as the fire fighters of cyberspace.

CSIRTs first came into existence in 1988, when one of the first internet worms travelled throughout the worldwide web and interrupted the activities of most systems.[4] That year, the first CSIRT

[3] UK Category 2 Responders, 2003. Generic Emergency Planning Arrangements for Telecommunications.

[4] Worm is a type of virus that disseminates itself inside the network.

archetype was developed and registered in the U.S. Patent Office; it is still functioning within Carnegie Mellon University. The CSIRT model was developed in the academic sector and proved to be successful. Today, CSIRTs have become the most important tool for managing information technology (IT) security incidents for electronic communications networks. Currently, there are several hundred CSIRTs of different sizes and affiliations, including national, commercial, and academic teams.

Under CSIRTs, managing security incidents is carried out in three basic stages (Moira et al., 2003):

1. Receive and evaluate incident reports and complete initial prioritization.
2. Study and technically handle the incidents and inform target groups of users about the threats.
3. Respond to, statistically register, and prevent the spread of incidents, and restore network function.

CSIRTs include IT security experts whose main objective is to respond to computer security incidents. These experts provide the necessary services to handle incidents and support their constituents recovery from breaches. To mitigate risks and minimize the number of required responses, most CSIRTs also provide preventative and educational services for their constituency. They issue advisories on vulnerabilities in software and hardware and inform users about exploits and viruses taking advantage of these flaws. Having a dedicated IT security team helps an organization mitigate and prevent major incidents and helps to protect its valuable assets. Further possible benefits are:

- centralized coordination for IT security issues within the organization (Point of Contact);
- centralized and specialized handling of and response to IT incidents;
- the expertise at hand to support and assist users to quickly recover from security incidents;
- support for dealing with legal issues and preserving evidence in the event of a lawsuit;
- resources to keep track of progress in the security field; and
- cooperation within the constituency on IT security (awareness building).

CSIRTs play an important role in crisis management because they operate 24 hours a day, 7 days a week; this kind of access may not be available within other critical infrastructure sectors. The UK's national Computer Emergency Response Team acts as an apex organization, coordinating incident countermeasures at the national level and supporting critical infrastructure companies. The team helps companies handle cyber security incidents, though some critical sectors have their own teams.

In the United States, CSIRT activities at the national level are performed by the Computer Emergency Readiness Team, which addresses incidents concerning United States national security. The United States also hosts specific CSIRTs acting in local sectoral networks as well as the Coordination Center, which is the center for the Software Engineering Institute. This center researches software flaws that impact internet security, publishes papers, and works with various stakeholders to improve the security of cyberspace as a whole. Other national CSIRTs include the Government National Cryptologic Center in Spain and the National Cyber Security Centre in Finland. All of them cover CIIP as well.

Observations and Recommendations Regarding Information Sharing and Incident Management

Information sharing, which is a horizontal process, is a cornerstone of CIIP. The following observations may be useful to consider when designing national information sharing practices.

Bi-directionality of information sharing: Good information sharing is a bi-directional, PPP-type activity that involves both the public and private sectors. It is a continuous effort that requires relationships be maintained with information sharing partners.

Trust and face-to-face communication: Experts in best practices emphasize that quality information sharing cannot be achieved without a high level of trust. Any electronic system dedicated to information sharing would not build that trust and must not replace good inter-personal relationships achieved through regular face-to-face meetings.

Electronic tools for information sharing in CIIP: When trust and relationships are maintained, electronic systems provide good facilitation of the processes and make it more efficient. In particular, electronic systems are efficient in cases of large CIP communities such as the EU and the United States. The authors emphasize, however, that electronic systems serve to facilitate information sharing but are not essential to the process.

Mandating information sharing: Practical collaboration in information sharing has proven that, first and foremost, it should be promoted as a voluntary process and that obligations in these areas usually have limited success. Legal tools mandating information sharing should be enacted to a limited degree and for well-defined purposes, for instance, in case of risk assessments and incident reporting. Mandatory incident reporting of large disruptions is mandated in the EU. Highly confidential information that needs to be shared must be regulated and captured by the relevant legal frameworks as the nature of the information tends to be sensitive from both commercial and security standpoints.

National risk assessment and national CIIP plan: Regular assessment of national risks helps shape strategic national CIIP priorities. While performing national risk assessment, countries are increasingly going beyond the risks that arise domestically to also include the international context. Different countries find themselves susceptible to different sets of risks—there is no "one-size-fits-all" set of threats. National risk assessment should lead to the preparation of a national CIIP plan that would aim to address and mitigate those dangers. Such a plan should provide clear guidance and allocate responsibilities for how security and reliability of the national critical infrastructure should be ensured, coordinate public–private initiatives, and initiate implementation review processes.

Regular critical infrastructure sector assessments and preparation of sectoral CIIP plans: Routine assessment of the resilience of each critical infrastructure sector to identify risks is a good practice as it monitors the state of critical infrastructure assets, gradually enhancing and adjusting resilience. Routine assessment could be integrated with sectoral CIIP plans. The authors recommend that this process be assigned to agencies that lead CIIP efforts for each critical infrastructure sector.

Managing security incidents: Incident management is one of the key elements of CIIP. Security incidents should be reported, investigated, and addressed in a timely manner. Cyber-attacks have an impact not only on the ICT sector, but are real threats to all critical infrastructures. The authors recommend that Computer Emergency Response Team activities be adopted systematically from the national level to the sectoral level for critical infrastructure operator networks. Such teams would improve the detection of and reaction to security events and the execution of responses.

Exercises: Simulation exercises are tools to understand and increase preparedness, and to detect possible gaps in security and resilience. These exercises build relationships and partnerships within the critical infrastructure community. The authors recommend that exercises be performed regularly at the national level as well as within sectors or between the interconnected sectors.

6

Current Status of CIIP in the LAC Region

Survey Methodology and Results at the Regional Level

One of the objectives of this study was to provide recommendations to Latin American and Caribbean (LAC) countries regarding critical infrastructure information protection (CIIP) framework development, taking into account the experiences of a select group of countries and one region. To better understand the situation in LAC, the authors conducted an electronic survey to assess the status quo. The survey purposefully focused on critical infrastructure protection (CIP) instead of CIIP to allow respondents to research and respond more easily.

All LAC countries were surveyed, and electronic questionnaires were developed separately for the public and private sectors. The online questionnaires were designed so many participants could be interviewed in a relatively short period of time. All the responses were stored in a database so information could be aggregated and analyzed using empirical and statistical methods. The public sector audience included government agencies, ministries, and other public institutions that are likely to be dealing directly or indirectly with governance of critical infrastructure sectors as well as computer security incident response teams (CSIRTs). The private sector audience included private and public companies that operate infrastructures that are likely to include critical infrastructure assets. Companies were selected randomly within a structure to ensure the participation of each critical infrastructure sector and service in each country. Table 6.1 includes critical infrastructure sectors and services that were surveyed. Representatives from the public and private sectors were asked to identify their critical infrastructure sector or service before beginning the survey.

The public sector questionnaire was designed to increase the awareness of the policy and governance framework for CIP. The survey included questions related to different aspects of a CIP framework: strategy, legislation, and responsible institutions; a list of identified national critical infrastructures; incidents; crises management; and public–private partnership (PPP) approaches.

The purpose of the private sector survey was to find out how companies that are likely to operate critical infrastructure assets are approaching security threats, dealing with incidents, and managing other CIP considerations. This survey included questions related to critical infrastructure operators' CIP practices such as risk assessment, methods of incident and crisis management, ways to identify threats to industrial systems, and how they protect and defend their assets. Additionally, participants were asked to provide examples of real incidents, budgets allocated for critical infrastructure security, and observations from results of security audits.

TABLE 6.1. Critical Infrastructure Sectors Surveyed

Critical infrastructure sectors and services	Subsectors
Information and communications technologies (ICT)	Telecommunications, internet service providers
Energy	Gas, petroleum fuels, refineries, pipelines, electricity generation, and transmission
Finance	Banking, finance, and trading exchanges
Food	Production, storage, and distribution
Emergency services	Emergency and rescue services, disaster response
Health	Hospitals, public health, and laboratories
Transport	Transport and traffic infrastructure, including air, road, sea, rail, and cargo distribution
Utilities	Water, waste water, and waste management
Defense	Military, law enforcement, national security, and public security
Government	e-Government infrastructure and services, public administration, parliament, and justice
Critical manufacturing	Country specific
Civil contingency	–
Space and research	–
Information services and media	–
Chemical and nuclear	–
National monuments and icons	–
Other	Surveyed representatives were given an option to choose “Other” if they do not belong to any of the above critical infrastructure sectors and services.

Source: Authors.

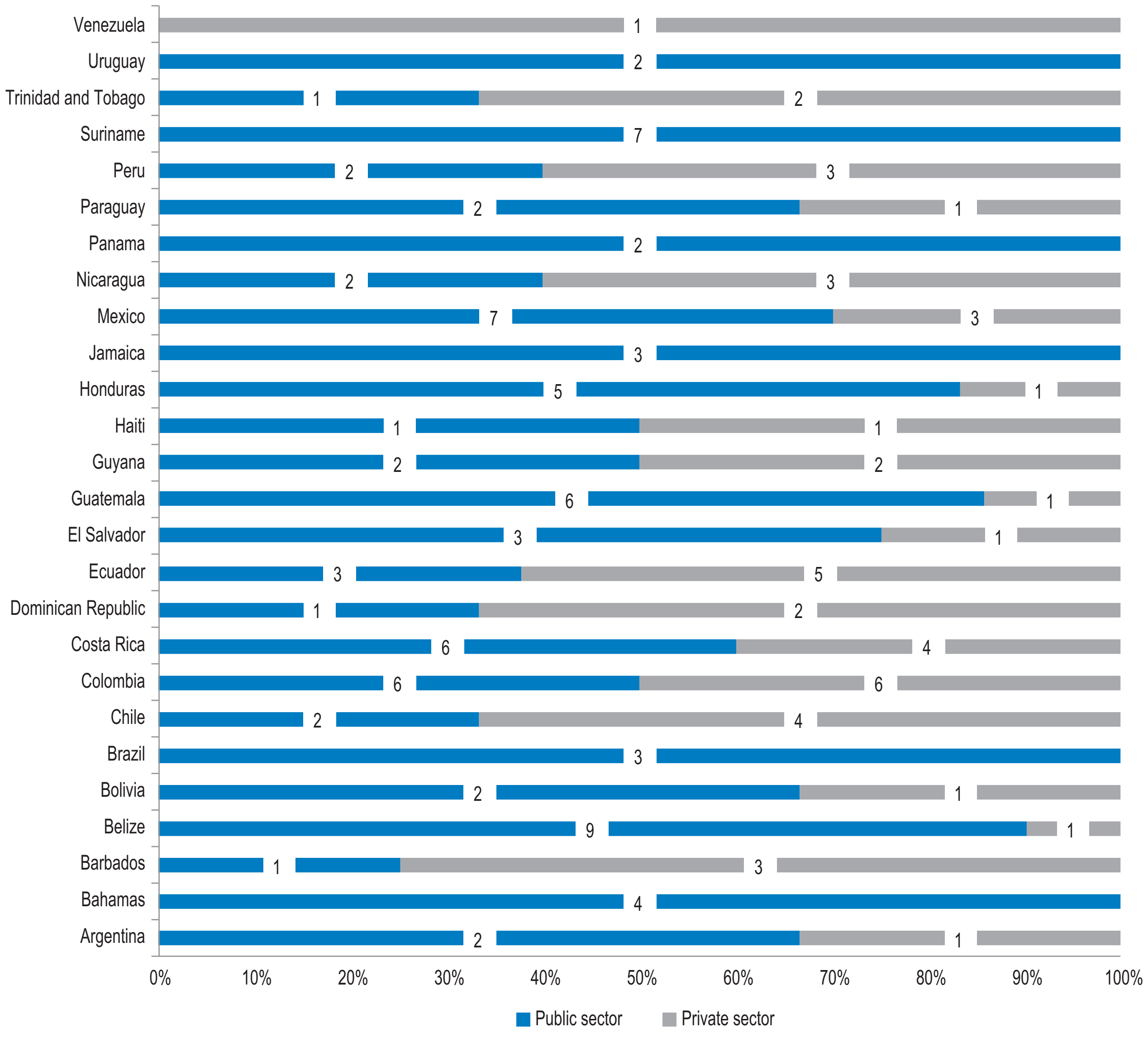
A total of 933 contacts were identified across the region within all of the critical infrastructure sectors and services. They were all invited to participate and 130 participants across all 26 countries completed the surveys. The 13.9 percent response rate should not be underestimated because the topic of CIP is relatively new to the region and some countries and stakeholders may be reluctant to share any type of sensitive information. The response rate might have been lower if the surveys had focused on CIIP.

The number of responses per country is provided in Figure 6.1. The following sections provide some regional-level insights derived from the completed surveys. Results of the survey were also used to understand CIP developments within each individual country. Where the response rate per country was higher (in 11 countries, there were five or more respondents), it was possible to derive more accurate conclusions than where the response rate was lower (in 15 countries, there were four or fewer respondents). For the countries with lower response rates, the information was still analyzed, including an additional cross-check of the information whenever possible; however, the clarity of national CIP development is less accurate and some inaccuracies may remain. Of note, each country was also included in a cluster, and the clusters were then analyzed.

In six countries, no private sector surveys were submitted. In eight countries, the private sector response rate was higher than that of the public sector, which could indicate awareness and engagement.

The authors note that the surveys were provided to the bodies (public and private) that were likely to have a role in governing or operating critical infrastructure assets but that the survey was entirely voluntary. Responses are a measure of a personal interpretation of facts and a subjective

FIGURE 6.1. Number of Responses Submitted per Country and per Sector



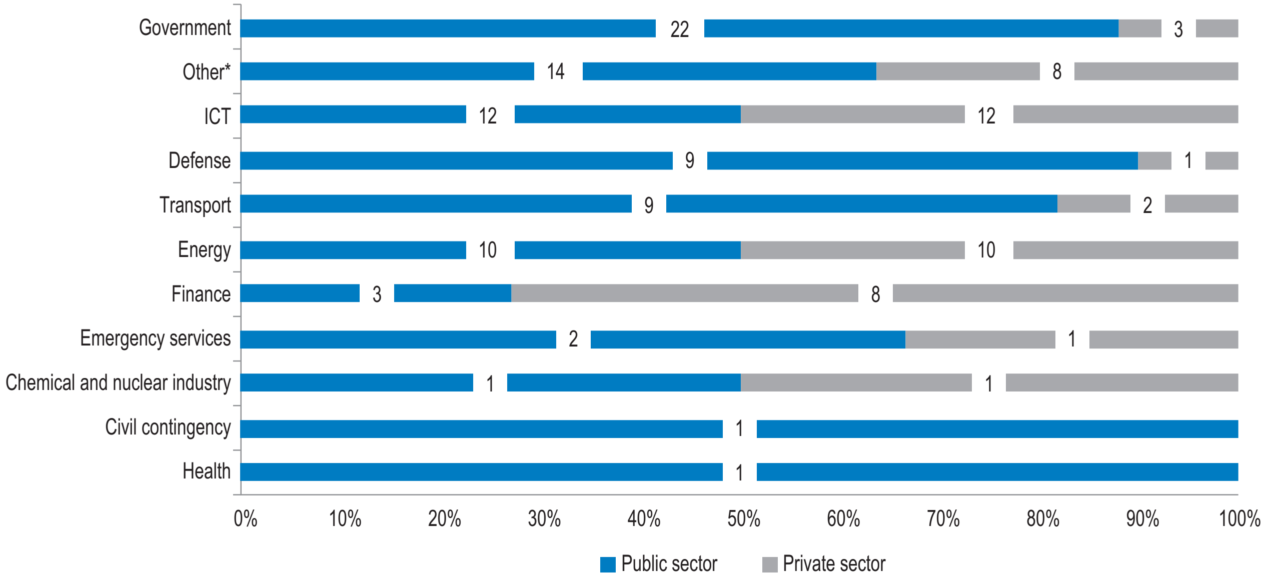
Source: Authors.

reflection of familiarity with CIP issues from the individuals filling in the questionnaires. As is typical of large-scale surveys, the accuracy of this research is not absolute and information should be treated with caution in relation to the actual CIP situation at the country level. Results of this research were aggregated using empirical and statistical methods. To achieve higher accuracy and precision, the authors recommend further research with onsite visits in individual countries; face-to-face interviews with CIP-related bodies, companies, and local experts; and exercises measuring CIP effectiveness.

Observations on CIP Framework Development at the Regional Level

The authors' analysis of the information from the completed surveys allowed them to summarize the CIP situation in LAC and to project similar results

FIGURE 6.2. Number of Responses per Critical Infrastructure Sector or Service

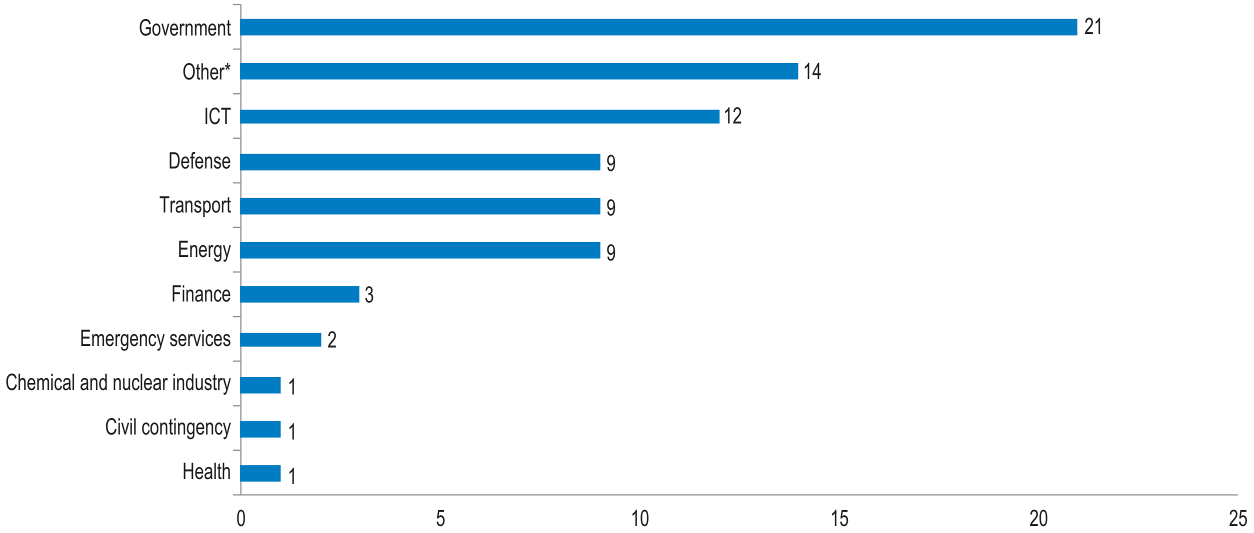


Source: Authors.

*A respondent may have chosen "Other" if they did not want to identify the critical infrastructure sector or service they represent. There were no respondents from the food, utilities, critical manufacturing, space and research, information services and media, or national monuments and icons sectors or services.

for CIIP. The sections that follow present the most prominent findings from the surveys for the public and private sectors. The authors note that the majority of responses across both sectors were received from the ICT, defense, finance, transport, and energy sectors (Figure 6.2).

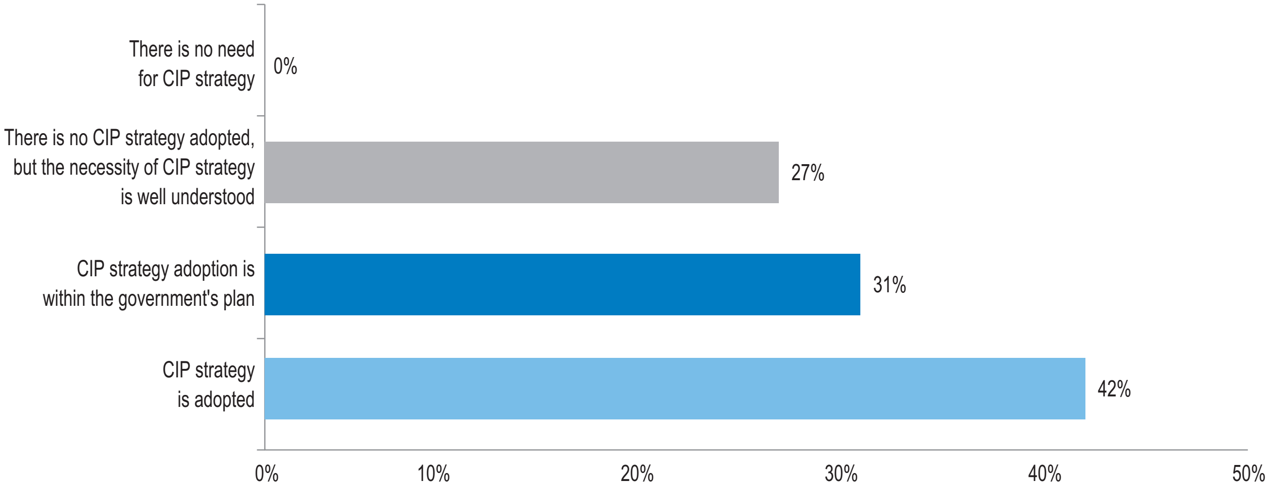
FIGURE 6.3. Number of Public Sector Respondents per Critical Infrastructure Sector or Service



Source: Authors.

*A respondent may have chosen "Other" if they did not want to identify the critical infrastructure sector or service they represent. There were no respondents from the food, utilities, critical manufacturing, space and research, information services and media, or national monuments and icons sectors or services.

FIGURE 6.4. CIP Strategy Adoption in LAC, 2015



Main Observations from the Public Sector Survey

In total there were 84 respondents to the public sector survey and the majority were provided by public organizations dealing with government services and infrastructure and the ICT, energy, transport, and defense sectors (Figure 6.3).

Survey results indicate that slightly above 40 percent of LAC countries have adopted a CIP strategy or that elements of CIP are integrated into the national security strategy (Figure 6.4). The positive result is the region-wide understanding of the need for a CIP strategy or the existence of plans to develop a CIP strategy. The current low CIP strategy adoption rate points to the gap between understanding the importance of addressing CIP issues and actual framework development.

Primary and secondary CIP legislation is not widely developed across the region, or at least information about legal CIP frameworks is not well known within the countries (Figure 6.5). Of the

FIGURE 6.5. Adoption of CIP Legislation in LAC, 2015

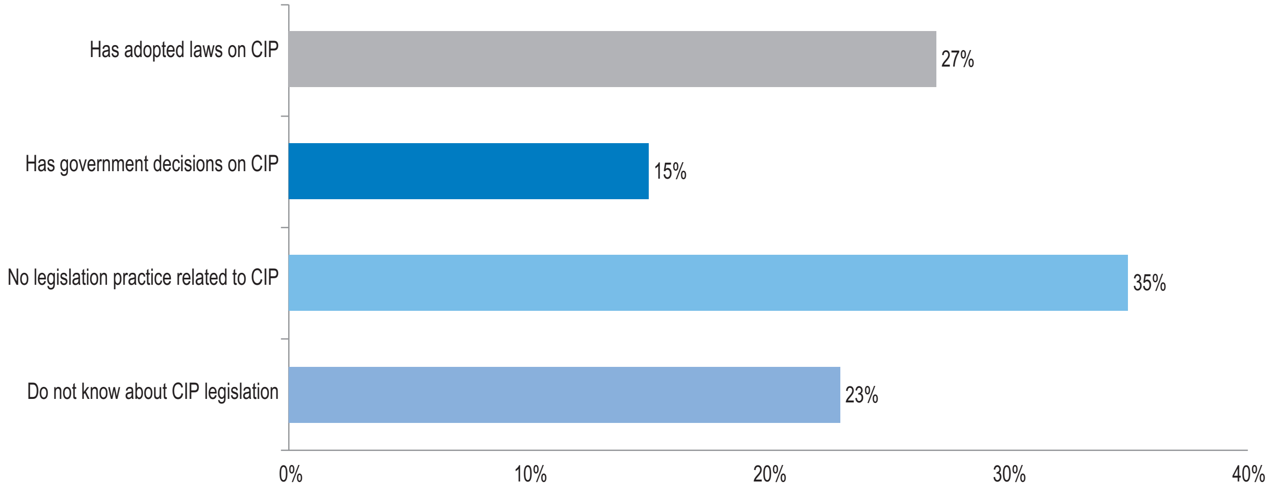
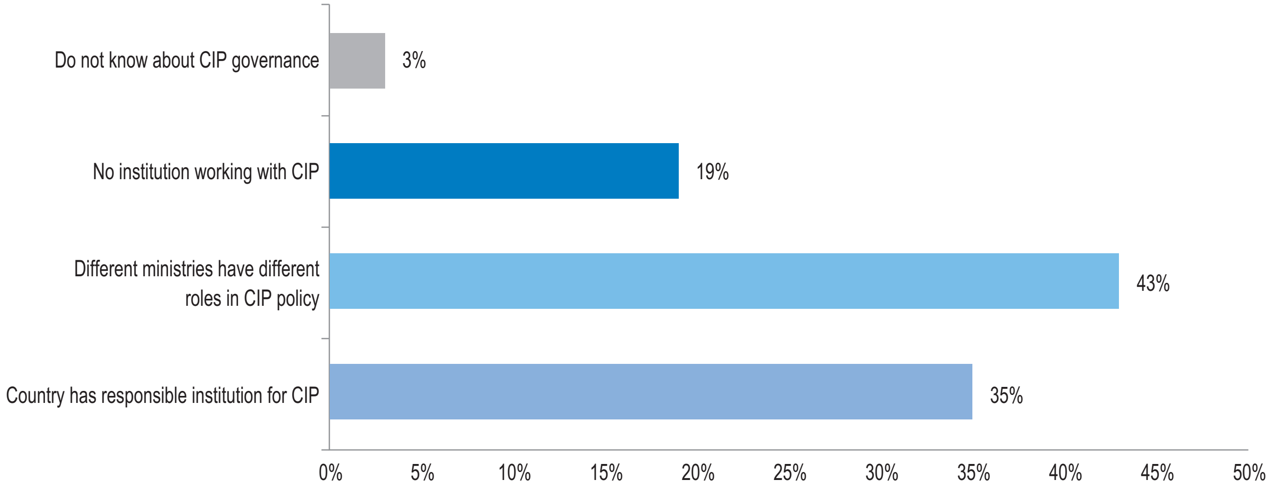


FIGURE 6.6. **CIP Governance Framework in LAC, 2015**



countries in the region, respondents from 35 percent reported no legislative practice in CIP and 23 percent were not aware of CIP legislation in their country. Respondents from only 27 percent of LAC countries reported that there were laws for CIP and 15 percent were aware of government decisions addressing CIP. These results indicate an important gap between the strategic planning of CIP activities and implementation of a CIP framework, including setting up relevant procedures and assigning responsibilities.

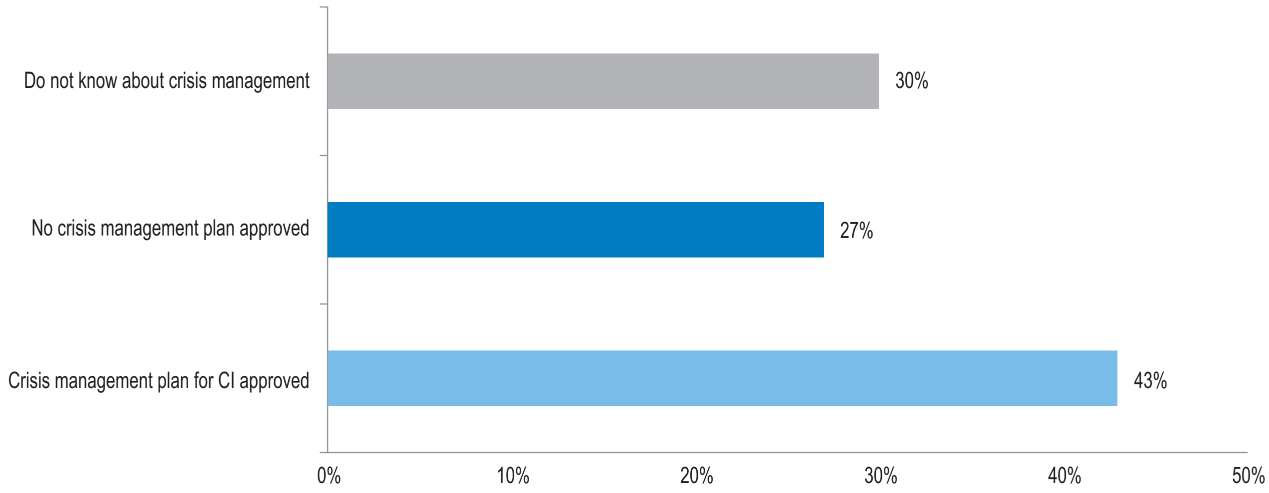
Regarding CIP governance models, the most common was the strategy whereby different ministries and agencies had different roles in CIP policymaking, administration, and management (43 percent) and only 35 percent of LAC countries were reported as having a dedicated government institution responsible for CIP. In the rest of LAC countries, respondents said there was no responsible body appointed (Figure 6.6).

When asked to list national critical infrastructure sectors and services, respondents were not consistent and in some instances participants within the same country provided different information. Lists of critical infrastructure sectors and services also varied among countries; however, variations were not significant, with respondents from most countries reporting transport, energy, government, healthcare, ICT, emergency services, and water. Those results correlate with international practices like those provided in Table 6.1. The finance, dams, food, critical manufacturing, and defense sectors were mentioned less frequently. The critical infrastructure sectors and services referred to least were chemistry, research, and nuclear and space. Based on these results, the authors concluded that critical infrastructure sectors and services are not clearly identified in each LAC country or at least that there is not sufficient awareness regarding identification. However, the authors did find good overall understanding of what critical infrastructure sectors should be on the national level.

Respondents from almost half of the LAC countries (43 percent) noted that crisis management plans had been adopted for critical infrastructure and 35 percent noted that their country evaluates and exercises those plans to keep them up to date. The responses show that crisis management is part of national emergency or defense frameworks. Unfortunately, most LAC countries were not seen as being properly prepared for crisis situations, with respondents from 27 percent reporting no crisis management plan in place and from 30 percent not being aware of such plans (Figure 6.7).

According to the findings, 35 percent of LAC countries require critical infrastructure operators to report security incidents to responsible authorities

FIGURE 6.7. Adoption of CIP Crisis Management in LAC, 2015



(e.g., CSIRTs) and five countries (19 percent) have established sanctions or penalties if a critical infrastructure operator does not report a security incident. Disruption types included natural disasters (earthquakes and hurricanes) in Belize, Mexico, and Chile; technical damage (electricity blackout, dam break, and internet cable damage) in Panama and Paraguay; and cyber-attacks in Ecuador and Belize. Moreover, respondents from another 35 percent of LAC countries reported that risk evaluations and physical and/or cyber vulnerability analysis was being done for critical infrastructures. They mentioned this practice is done mostly within public institutions and the financial, electricity, and telecommunications sectors.

Respondents from the majority (65 percent) of LAC countries claimed governments cooperate with the private sector for CIP. This is a positive indication that could lead to improving CIP in each country and in the region.

Main Observations from the Private Sector Survey

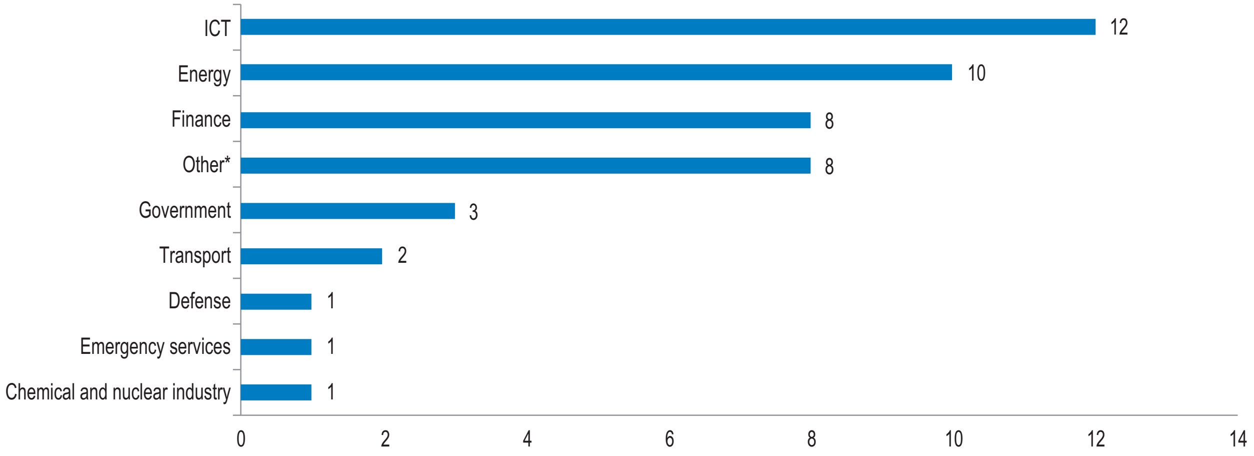
In total, 46 public and private companies operating in critical infrastructure sectors were surveyed. The most active were companies operating in the energy, ICT, and financial sectors (Figure 6.8).

Of the surveyed companies, 54 percent identified parts of their assets as critical infrastructures. The same proportion of organizations reported having crisis management plans for operated critical infrastructure assets (Figure 6.9). When asked to name managed critical infrastructure assets, most of the companies referred to IT infrastructure, communications networks, and SCADA systems. From the information provided, the authors observed that understanding critical infrastructure assets is largely limited to the IT and communications components of operated infrastructures. This means that critical infrastructure is likely perceived as critical information infrastructure (CII), which is not accurate and excludes many non-ICT critical infrastructure assets.

At the same time, as much as 40 percent of surveyed companies reported not performing regulated risks assessments for cyber threats applicable to critical infrastructure (Figure 6.10). In the context of rapidly increasing cyber-attacks and espionage incidents, this is a high risk. Companies that reportedly assess cyber threats indicated doing so every two years. In the constantly changing environment of cyber threats, a two-year interval is probably not frequent enough.

Only 33 percent of companies surveyed take into account security risks when reviewing the

FIGURE 6.8. Number of Responses Provided by Private Sector Representatives per Critical Infrastructure Sector or Service

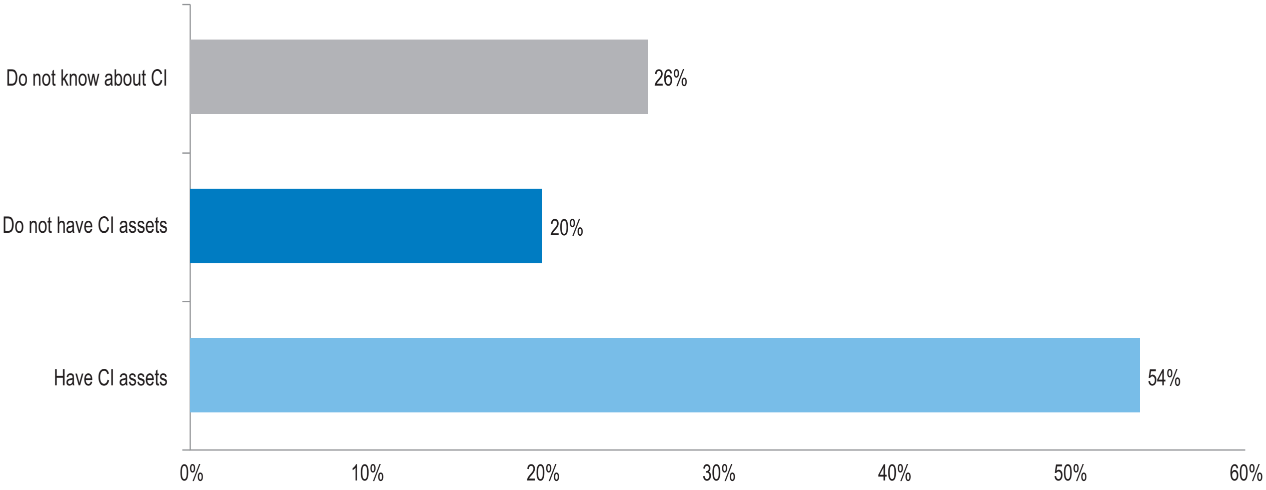


Source: Authors.
*A respondent may have chosen "Other" if they did not want to identify the critical infrastructure sector or service they represent. There were no respondents from the food, utilities, critical manufacturing, space and research, information services and media, national monuments and icons, health, civil contingency, or chemical and nuclear industry sectors or services.

stability of the organization's Industrial Control System (ICS) and SCADA. Only 28 percent still have an impression that security is not an issue for ICS and SCADA because it is supposed to be an isolated system by design (Figure 6.11). In this regard, 23 percent of companies registered an increase in incidents targeting the ICS and SCADA systems during the past year, while only 5 percent registered a decrease in such incidents. When asked to measure financial losses from such incidents, companies reported the measured impact within the range of several thousand U.S. dollars to at least to $200,000.

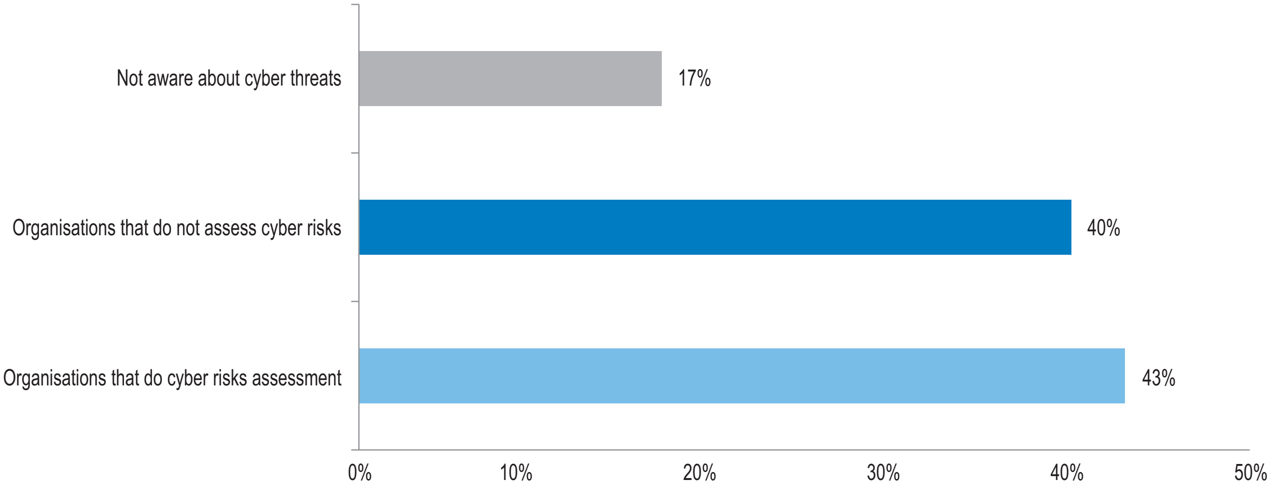
The majority of responses reveal that cyberattacks are considered the main threat for critical infrastructures. Respondents indicated that

FIGURE 6.9. Critical Infrastructure Assets Managed by Companies in LAC



Source: Authors.

FIGURE 6.10. Assessment of Cyber Risks by Companies in LAC



their companies were investing in cyber detection, defense, and confidential information protection, where critical infrastructure operators specified firewalls, malware detection, and intrusion prevention/detection systems as the most frequently used tools. Respondents also identified risks related to the reliability of critical infrastructure systems such as electricity supply, backup systems, human resources management, authentication of users accessing critical infrastructure, redundancy, and duplication of critical elements.

When it comes to information sharing practices, 48 percent of respondents would support sharing risk information related to CIP with external stakeholders such as regulators, government bodies, or banks, but 28 percent opposed that idea.

Methodology and Criteria to Cluster LAC Countries

While this study did not aim to provide per-country recommendations, the authors still attempted to

FIGURE 6.11. Perception of Security Risk Related to ICS and SCADA

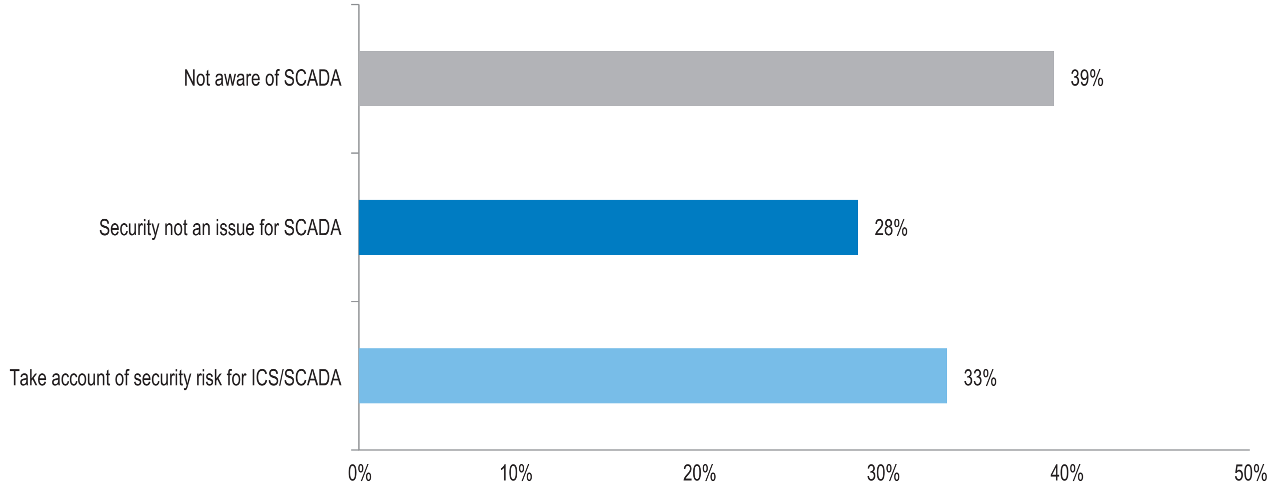


TABLE 6.2. Four Stages of CIP Policy and Governance Model Development

	CIP policy and governance model development
Stage 4	• National CIP efforts are guided by the national strategy. • CIP-dedicated primary and secondary legislative acts are adopted. • CIP responsibilities and functions are explicitly formulated and linked to instructions. • CIP strategy implementation plan is adopted with descriptions of specific measures. • PPP model for CIP (including a national Computer Emergency Response Team, or CERT) is in place. The countries in this category are mostly advanced in CIP policy and governance. They have taken specific measures to manage CIP at a national level, have a dedicated budget to improve the protection of critical infrastructure assets, and have developed a working plan to implement CIP policy.
Stage 3	• A general framework for CIP is in place, including policy and legislation. • Implementation of CIP measures is fragmented. The countries in this category have a CIP strategy, legal acts, and responsible ministries, but national supervision is weak, usually with only CERTs actively involved.
Stage 2	• CIP policy is part of the national defense system. • CIP importance is understood, but the framework is not systematically organized. The countries in this category have acknowledged the importance of CIP for national defense and have incorporated CIP into the national security plan; however, the definition of national security does not incorporate economic security. These countries do not address CIP as part of national policy with special attention to cyber threats (CIIP).
Stage 1	• No clear activities related to CIP policy or governance model development. The countries in this category have no systematic organization of CIP at the national level and no clear legal basis for CIP.

Source: Authors.

tailor recommendations to national CIP development. With that objective, the countries were clustered into four groups based on two criteria: (1) level of development of CIP policy and governance and (2) level of critical infrastructure identification and protection. The authors note that currently there is no single regional or global source for CIIP-related information. Therefore, this study is one of the first attempts to understand CIP readiness at the regional level, including gaining some insight into the level of CIP awareness across the different public and private stakeholders. Taking this into account, the results of the survey were used to understand CIP development within each country in the region and served as a basis for clustering.

The first criterion examined the level of CIP policy and governance model development as well as the established CIP framework for each country. CIP activities should be guided by a CIP policy and legal framework and be performed within the existing governance structure. A well-established CIP framework is thus a cornerstone for consistent improvement in CIP in a country. Table 6.2 provides descriptions of four stages of CIP policy and governance model development that were used to cluster the countries. Indeed, CIP efforts can be successful only when they are collaborative across all stakeholders and within an environment that is highly aware and supportive. Thus, criteria used to assign countries to a particular stage are more qualitative than quantitative. The authors needed to establish not only the presence of CIP strategy (and other level acts), but also to evaluate the level of awareness of a national CIP framework and an understanding of its relevance. In some countries, responses were more numerous and aligned, while in other countries, not only were the responses less numerous, but also contradictory, signaling a lower level of awareness and engagement.

The second criterion was designed to capture the work performed so far related to identifying and protecting critical infrastructure assets. It reflects implementation of an existing CIP framework. As with the previous criterion, four stages were defined (Table 6.3).

TABLE 6.3. Four Stages of Critical Infrastructure Identification and Protection

	Critical infrastructure identification and protection
Stage 4	• Specific criteria to identify critical infrastructure assets are established. • Program to implement critical infrastructure security measures is working. The countries in this category are mostly advanced in CIIP and have implemented specific measures to identify and protect critical infrastructure assets.
Stage 3	• The overall framework to identify critical infrastructure sectors is established. • Identifying and cataloguing critical infrastructure assets is in progress. The countries in this category have a methodological approach to identifying critical infrastructure assets and services, with specific steps and responsibilities assigned to stakeholders.
Stage 2	• Identification of critical infrastructure sectors is performed. The countries in this category have acknowledged some critical sectors to maintain vital societal functions.
Stage 1	• There is no systematic approach to identify critical infrastructure sectors. The countries in this category have no system to identify critical infrastructure.

Source: Authors.

Clustering by these criteria reflects how a particular country deals with critical infrastructure and what level of maturity it has achieved. These maturity levels range from the absence of activities to identify critical infrastructure assets (Stage 1) to the presence of well-established measures to specify critical infrastructure assets (Stage 4). For instance, countries that were reviewed as best international benchmarks in the previous sections of this book could be associated with the most advanced stage.

The following section reviews national CIP efforts and provides results from clustering. Countries were clustered on the two criteria separately since countries could be in different stages for each criterion. This approach allowed the authors to adjust to the needs of each country, therefore possibly better directing national CIP efforts.

Review of CIIP Efforts across LAC Countries and Clustering

Based on the analysis of the information collected, the authors concluded that disparities in the maturity of CIP frameworks across LAC are significant. Major differences were observed in the level of CIIP policy making, governance, and approach to critical infrastructure identification.

Stage 3: Argentina, Brazil, Chile, Colombia, and Mexico

None of the LAC countries reached the level of CIIP that could be associated with Stage 4. Five countries—Argentina, Brazil, Chile, Colombia, and Mexico—demonstrated notable efforts in CIIP framework development and implementation.

Argentina, for instance, identified critical sectors and adopted its National Program for Critical Information and Cybersecurity Infrastructure (ICIC)[1] in 2011. Protecting critical infrastructure assets is covered by separate legal acts (e.g., the penal code). The National Directorate of CII and cyber security coordinates national CIP efforts, while sector ministries implement sectoral CIP competencies. The ICIC's critical infrastructure group (ICIC-GICI) surveys, identifies, and classifies CII , while its administrative arm (ICIC-CERT) reviews the reports and works to find solutions to cyber incidents targeting national critical infrastructure.[2] Since 2012, Argentina has performed annual exercises to strengthen protection and

[1] See http://www.icic.gob.ar/.

[2] https://www.first.org/members/teams/icic-cert.

readiness of national critical infrastructure. More information about Argentina's approach to CIIP is provided in Appendix 2, which features the country's national case study. Notwithstanding good overall CIP efforts, the number of survey responses received from Argentina was low (three in total; one from the public and two from the private sectors). Yet, the information about their CIP framework and activities is well structured and available online. Among the reasons for low participation may have been an unwillingness to share information related to CIP, but it could also indicate low awareness of the subject at the national level.

In Brazil, the critical infrastructure sectors are identified; however, current practical activities related to CIP are oriented toward ICT. Different elements of a CIIP framework are covered by strategic documents regarding civil defense, a growth acceleration program, and an electronic government program.[3] At the level of the legal acts, criminal law, a cybercrime bill, and the penal code mainly address CIIP. The Institutional Security Cabinet and the Ministry of Planning coordinate CIIP efforts at the national level, while other institutions such as sectoral ministries (e.g., the Ministry of Science and Technology and the Ministry of Communication) are assigned relevant CIP competencies. The national CERT responds to cyber incidents targeting critical infrastructure, while the CSIRT deals with incidents that affect networks that belong to the federal public administration. Brazil has established a multistakeholder organization for cooperation in CIIP, the Brazilian Internet Steering Committee. As in Argentina, the number of responses from Brazil was only three and public sector institutions provided all of them. Also, survey responses were somewhat contradictory, which may signal uneven awareness of CIP efforts across public bodies in Brazil. None of the private companies that were contacted responded, which may indicate an unwillingness to share information related to CIP, but it may also indicate a low level of engagement.

Chile's CIP legal framework is well developed at the sectoral level. Critical infrastructure sectors are identified and relevant actions have been taken to strengthen identified critical infrastructure assets (Box 6.1). Legislation was adopted to address states of emergency caused by nature and human or productive activities. Regulations to protect, recover, and continue telecommunications critical infrastructure were adopted in 2012. The National Emergency Office and the Chilean Armed Forces have roles in CIP crisis situations, as does the Committee for Cyber Security, which was created to prepare a national cyber security policy. Telecommunications operators are obliged to report incidents, and the country's CSIRT is responsible for the governmental sector, including responsibility for CIIP. There were six respondents to the surveys from Chile (two from the public and four from the private sectors), which suggests a good level of awareness in general and particularly in the private sector. This level of response is a positive sign that companies are engaged in CIP, which is essential for successful implementation.

In 2014, Colombia defined critical infrastructure sectors and began identifying critical infrastructure assets by collecting relevant information from critical infrastructure operators. A national digital catalog of critical infrastructure assets was completed in 2015. The country has a well-established disaster and risk management approach and is recognized as a regional leader (Box 6.2). Recently, Colombia updated its National Plan for Disaster Risk Management for 2013–25 and adopted a cyber security and defense strategy. The Ministry of National Defense is responsible for coordinating national activities for CIP. Other institutions involved in CIIP are the Joint Cyber Command and the Policy Cyber Center. Colombia's CERT is reacting to cyber incidents within the government sector. CSIRT-CCIT is a national team for all types of cyber incidents. Moreover, Colombia has established a PPP working group on CIIP. The financial sector makes an effort to evaluate risks and protect critical infrastructures. Unlike in Argentina

[3] http://www.defesa.gov.br/arquivos/estado_e_defesa/livro_branco/lbdn_2013_ing_net.pdf.

Box 6.1. Sectoral CIP in Chile

The history of disasters in Chile has led to the adoption of legal measures to reduce risk and respond to disasters. However, Chile has no strategy specifically for CIP generally—critical infrastructures are being protected at the sectoral level. This work has led to notable improvements in critical infrastructure resilience and robustness, particularly in the telecom sector.

In February 2010, Chile faced a strong earthquake (8.8 on the Richter scale) that affected a large part of the vital telecommunications infrastructure, damaging communications, both commercial and emergency services. At that time, this type of infrastructure was not regulated by the state as critical, meaning there were no standards established for minimum energy autonomy or capacity extension for communication channels. After the earthquake, Chile undertook important legal reform, identifying critical infrastructure assets within the telecom sector and establishing a set of minimum requirements to improve the robustness of and protect those assets.

Results of this work were observed after the earthquake in September 2015. The country's critical telecommunications infrastructures were not damaged, and internet, radio, and television services operated smoothly. Some outages were reported due to a fault in electricity supply.

In the Energy sector, in 2012, Chile established the Undersecretary of Energy's Domestic Energy Security Committee whose role is to advise on relevant actions in case of a disaster that affects the energy supply. Additionally, the country has undertaken exercises to test communication protocols with public entities, electric companies, and the hydrocarbons sector.

Overall, Chile's national electricity system serves around 1,500 companies, and corporate consumers of energy were identified as priority (critical) installations and registered by the Ministry of Energy in the Priority Energy Installations of Information Systems. These installations must regularly update relevant information for coordination purposes. They must also maintain required facilities in case of an emergency affecting energy supply, such as maintaining appropriate backup energy systems, taking into account the population served.

Source: Authors.

Box 6.2. Colombia's Risk and Disaster Management Framework

In LAC, Colombia has established itself as a leader in developing a comprehensive vision for risk and disaster management. Colombia's advanced system is anchored on investments in structural measures, risk assessments, early warning and emergency response, institutional support, and financial and fiscal measures at the national and municipal levels, as well as the organization of national and local entities for emergency response.

The country's long history in organizing and designing risk management measures started with instruments such as the National System for Disaster Prevention and Response (1985) and the National Plan for Disaster Prevention and Response (1998). Recently, Colombia approved a new national policy and a *National System for Disaster Risk Management Law* 1523 (2012) that reflects a paradigm shift in which disaster risk management is explicitly recognized as a part of the development process. Also the law provides stronger incentives for local governments to invest in risk reduction and strengthen technical assistance.

Source: World Bank (2014).

and Brazil, respondents to the survey in Colombia represented both the public and private sectors. In total, 12 responses were received from Colombia, of which six were from public agencies and six were from the private sector.

In Mexico, critical infrastructure is defined as strategic within the *General Civil Protection Act*. The National Security Council governs CIIP, while line ministries are involved at the sectoral level. The Technical Secretary of the National Security Council reports on the National Risk Agenda and the country's inventory of strategic infrastructure (see Appendix 6 for the case study on Mexico's approach to CIIP). Increasingly, the country is focusing on cyber risks. Identification of CII assets is addressed using a dedicated methodology and rules established in the administrative manual of general application in the field of ICT, and information security. Mexico's CERT manages cyber-attacks on critical infrastructure. CIIP policy is addressed through the *National Security Law* and the National Digital Strategy. Secondary legislation and the penal code also cover cyber security issues. The Expert Committee on Information Security was created to coordinate CIIP. The National Center for Cyber Incident Response was created to respond to attacks on the technological assets of critical infrastructure. There were 10 respondents to the surveys from Mexico, of which the majority, seven, were submitted by the public sector. The authors note, however, that answers from different stakeholders were contradictory in a number of instances, which may signal that raising awareness in the public sector may be beneficial.

Stages 2 (Framework) and 3 (Identification): Bolivia and Panama

Two countries—Bolivia and Panama—have developed CIP frameworks and defined critical infrastructure sectors, but need to advance the identification of specific critical infrastructure assets. Both countries are therefore in the Stage 3 cluster for CIP framework development and in Stage 2 for critical infrastructure identification. There were fewer respondents from Bolivia (three) and Panama (two). Only public sector surveys were submitted from Panama.

In Bolivia, law defines critical sectors. The approach to CIIP framework development is based on risk evaluation. The National System for Risk Reduction and Disaster and/or Emergency Response has been adopted and structured in three territories (see Appendix 3 for the case study on Bolivia's approach to CIIP). Bolivia's national CSIRT is under the auspices of the Agency for Development of the Information Society in Bolivia; operations began in 2014. Since 2015, the Center for Computer Incidents Management under the Agency of Electronic Government and Information Communications Technologies has initiated incident management for the public sector.

In Panama, the National Strategy establishes critical infrastructure sectors for cyber security and critical infrastructure protection. The Authority for Public Services of the Republic of Panama regulates and monitors utilities and critical infrastructure in the water, sewerage, electric power, telecoms, television, and natural gas sectors. Other institutions in charge of CIP are the National Authority for Government Innovation and the National System of Civil Protection. Incidents targeting critical infrastructure are reported to the Authority for Public Services and CSIRT Panama. There is a PPP working group for CIP.

Stage 2: Costa Rica, Ecuador, and Peru

Costa Rica, Ecuador, and Peru have some elements of CIP frameworks in place. Respondents did not identify many systematic sectoral initiatives to identify critical infrastructure assets. All three countries are grouped in Stage 2 for CIP framework development and Stage 2 for critical infrastructure identification.

According to the information submitted through the surveys, in Costa Rica, current activities related to CIP mostly focus on CIIP. Costa Rica declared its intention to develop a National Cyber

Security Strategy following the Inter-American Cyber Security Strategy. The *Law for the Protection of Personal Data* partly covers matters related to cyber security. The Ministry of Science, Technology, and Telecommunications is the authority in charge of cyber security. In 2012, a Costa Rican CSIRT was created under this ministry to respond to cyber incidents that affect the government sector. There were 10 respondents from Costa Rica, with the majority (six) from the public sector.

In Ecuador, CIIP coordination is assigned to the National Secretariat of Public Administration and the National Secretariat for Risk Management. Respondents noted that the country performs exercises to strengthen its disaster management capacity and coordination. The country has plans to advance development of electronic government, which will require strengthening of CIIP in the public sector. There were eight respondents from Ecuador, of which five were from the private sector.

In Peru, the Ministries of Energy, Transport, and Defense are involved in CIIP. There is a PPP working group on CIIP. Private sector companies provided examples of practices to determine critical infrastructure, preparations for crisis management, and mechanisms to protect critical infrastructure. There were five respondents from Peru, three of which were from private companies.

For all three countries, the authors note that there is a good level of awareness regarding the national status quo and engagement in CIP within the public and private sectors. Both factors could support the countries' efforts to advance the CIIP agenda.

Stages 2 (Framework) and 1 (Identification): Belize, Dominican Republic, Guatemala, Guyana, Jamaica, Paraguay, and Uruguay

In seven countries—Belize, Dominican Republic, Guatemala, Guyana, Jamaica, Paraguay, and Uruguay—respondents identified certain elements of CIP framework. However, the authors could not recognize a systematic approach to identifying critical infrastructure sectors. The authors clustered these countries in Stage 2 for CIP framework development and Stage 1 for critical infrastructure identification.

In Belize, critical infrastructure sectors are mentioned in separate legal acts such as the *Telecommunications Act*, the *Electronic Evidence Act*, the *Electricity Act*, and the *Public Utilities Commission Act*. The Ministry of National Security; the Ministry of Finance; the Ministry of Energy, Science, and Technology; and the public utilities have roles in CIIP. The National Emergency Management Organization approved crisis management plans for some types of national emergencies such as hurricanes. Cyber threats are recognized as important risks to critical infrastructure, in particular the ICT market.

In the Dominican Republic, the National Development Strategy includes some aspects related to CIIP. The Office for the Development of Information Technology and Communication has a role in strengthening cyber security.

In Guatemala, CIIP is partly mentioned in the National Plan for Integrated Risk Management and the National Reconstruction Plan. Elements of critical infrastructure are covered by separate legal acts, including the *Law on National Coordinator Disaster* and the *Law of the National Security System*. The National Coordinator for Disaster Reduction takes part in the CIIP management process.

In Guyana, the Ministry of Home Affairs intends to work on cyber security. The Civil Defense Commission is responsible for crisis management and periodically evaluates readiness for natural disasters such as floods. Guyana's CSIRT has responded to information regarding security incidents of national importance since 2013.

Jamaica's Cyber Security Strategy was adopted in 2015. It aims to increase the resilience of CII systems. The Ministry of Water, Land, Environment, and Climate Change is responsible for policymaking, administration, management, and resilience for water. The Ministry of Transport, Works, and Housing has the same responsibilities for traffic systems.

Paraguay's CSIRT has been active since 2012. The government is developing a national cyber security plan.

Uruguay plans to advance development of electronic government, while the country's CSIRT coordinates protection of the state's CII assets.

The authors identified very limited information regarding CIP from the electronic surveys from the Dominican Republic, Jamaica, and Paraguay since there were only three respondents from each country, and there were only two respondents from Uruguay. In Uruguay and Jamaica, only the public sector filled in the survey. There were four respondents from Guyana: two from the public and two from the private sectors. Belize and Guatemala demonstrated a good level of awareness of CIP, particularly across the public sector. Of the 10 respondents from Belize, 9 were from the public sector. Seven respondents from Guatemala were from the public sector and a further eight were from the private sector.

Stage 1: Bahamas, Barbados, El Salvador, Haiti, Honduras, Nicaragua, Suriname, Trinidad and Tobago, and Venezuela

The Bahamas, Barbados, El Salvador, Haiti, Honduras, Nicaragua, Suriname, Trinidad and Tobago, and Venezuela were clustered in Stage 1 for both criteria, meaning that most of the work required for CIP is still ahead.

In the Bahamas, the Ministry of Public Works is examining the CIP issue and the National Emergency Management Agency has a role in crisis situations.

In Barbados, the CSIRT coordinates defense against cyber-attacks. Though private sector companies identify critical infrastructure, prepare for crisis management, and have mechanisms to protect critical infrastructure, no respondents reported activities to develop CIP policy or protect critical infrastructure at the national level.

Similarly, respondents from El Salvador noted an absence of activities related to developing a national CIP policy. The Directorate of Civil Protection and the Ministry of Environment have competencies in CIP.

According to the information submitted by Haitian respondents, government bodies are discussing CIP legislation and the establishment of a national CSIRT with the private sector.

In Honduras, the Ministry of Infrastructure and Public Services and the Ministry of Energy have competencies in CIP. Respondents noted that some risk assessment activities are performed in the energy, finance, and transport sectors.

Nicaragua's main CIP authority lies within the country's defense sector bodies. However, telecommunications companies do perform risk evaluations and monitor the security of critical infrastructure assets.

In Suriname, the Ministry of Defense, the National Bureau for Security, and the Central Intelligence and Security Agency have competencies in CIP. National coordination for crisis and disaster is under the auspices of the Ministry of Defense and the National Coordination Centre for Disasters.

Respondents from Trinidad and Tobago reported an absence of activities related to CIP policy development and protection of critical infrastructures at the national level. The national CSIRT coordinates defense against cyber-attacks. Respondents from private sector companies indicated that cyber incidents threaten their critical infrastructures.

Similarly no specific activities related to CIP were noted in Venezuela. Nonetheless the government CSIRT is handling cyber incidents targeting national critical infrastructures.

There were a good number of respondents from Suriname (seven), Honduras (six), and Nicaragua (five). There was less participation from the Bahamas, Barbados, and El Salvador, with four respondents each. Three contributions were received from Trinidad and Tobago, two from Haiti, and one from Venezuela. In Barbados, Nicaragua, Trinidad and Tobago, and Venezuela, the majority of responses were provided by the private sector; there were no contributions from the private sector in the Bahamas or Suriname.

TABLE 6.4. Consolidated Results of Clustering of LAC Countries for Two Criteria

Criteria	Level of CIIP policy and governance model development	Critical infrastructure identification practice
Stage 4	No Countries	No Countries
Stage 3	Argentina, **Bolivia**, Brazil, Chile, Colombia, Mexico, **Panama**	Argentina, Brazil, Chile, Colombia, Mexico
Stage 2	**Belize**, Costa Rica, **the Dominican Republic**, Ecuador, **Guatemala**, **Guyana**, **Jamaica**, **Paraguay**, Peru, **Uruguay**	**Bolivia**, Costa Rica, Ecuador, **Panama**, Peru
Stage 1	Bahamas, Barbados, El Salvador, Haiti, Honduras, Nicaragua, Suriname, Trinidad and Tobago, Venezuela	Bahamas, Barbados, **Belize**, **the Dominican Republic**, El Salvador, **Guatemala**, **Guyana**, Haiti, Honduras, **Jamaica**, Nicaragua, **Paraguay**, Suriname, Trinidad and Tobago, **Uruguay**, Venezuela

Source: Authors.

Consolidated Clustering Results

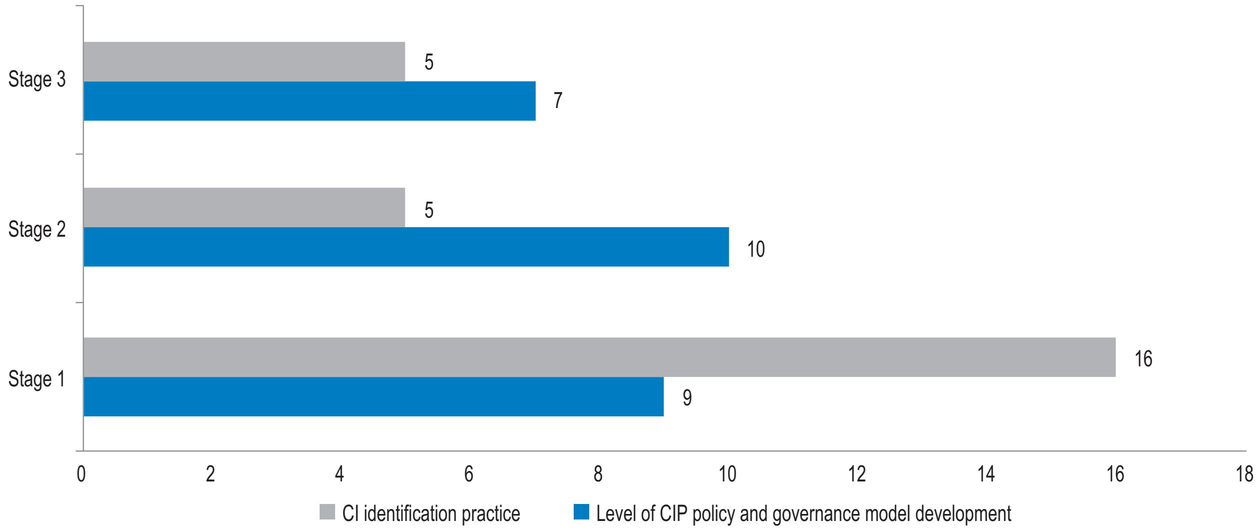
Table 6.4 provides the consolidated clustering results for the two criteria. Countries that were classified in two different stages are in bold.

Figure 6.12 shows that the majority of Stage 2 and 3 countries (of which there are 17) have undertaken certain steps toward developing a CIIP framework and establishing a governance model. Further efforts are needed to develop legal frameworks to regulate efforts to protect critical infrastructures. It is also obvious that the majority of countries in Stage 1 (there are 16) still need to undertake efforts to identify critical infrastructures, thus more work needs to be done to systematically identify critical infrastructure sectors and move toward identifying and cataloguing critical infrastructure assets.

Observations and Recommendations

In general, the LAC countries included in Stage 1 have a poor basis for CIIP. These countries have no practical approach in place to address CIIP, have made no progress (and sometimes have no motivation) in initiatives to secure and strengthen national critical infrastructures, and have not formally defined critical infrastructures. The key recommendation for that cluster is to build awareness

FIGURE 6.12. Number of Countries by Stage



Source: Authors.

and capacity related to CIIP within the public sector. This should help change the mindset and motivate and initiate CIP framework development.

Countries clustered in Stage 2 understand the importance of CIIP and have addressed CIIP issues in one way or another. However, attempts are mostly fragmented, distributed between ministries, and there is no systematic approach at the national level or it is not fully implemented. It is highly probable that ongoing support for this cluster would advance CIP framework development and boost the resilience of critical infrastructures significantly.

Stage 3 encompasses LAC countries that stand out from the others because of the maturity of CIIP work performed. Although these countries have resources and practices in CIIP, there remain important gaps within their CIP frameworks and implementation efforts. This is why no LAC countries were classified as Stage 4, which represents best practice countries that were analyzed within the context of this study.

Table 7.1 in the next chapter provides a consolidated list of the recommendations that LAC countries may find useful to implement. Not all of the recommendations are equally relevant for all of the countries since they depend on the current level of CIP framework maturity. The relevance of each recommendation is emphasized separately. As countries advance toward Stage 4, certain recommendations become less relevant. Alternatively, it may be too early for some recommendations for countries in the early stages of CIP framework development

7

Recommendations

This chapter provides a consolidated list of recommendations for CIIP framework development and implementation. The relevance of each recommendation is demonstrated as follows: '+' for low relevance; '++' for significant relevance; and '+++' for high relevance. Low relevance means, for countries currently at this stage, the recommended activity has already been performed or should be performed at a later stage.

TABLE 7.1. Consolidated List of Recommendations

		Clusters and relevance			
No.	**Recommendations**	**Stage 1**	**Stage 2**	**Stage 3**	**Stage 4**
a. Policy and Governance					
1.	**Prioritize CIIP at the national level**: Preparing and implementing a CIIP framework requires significant involvement of the public and private sector as well as dedicated financial resources and participation of academia. A significant level of engagement can be achieved by prioritizing the CIP agenda at the national level by developing primary national strategies such as the national security strategy.	+++	+++	++	+
2.	**Overarching framework for CIIP**: CIIP involves many sectors and actors from both the public and private sectors. CIIP policies and legal frameworks benefit from a single overarching policy document that encompasses all related areas and actions and establishes the governance framework. Such a document creates a full picture of the CIP framework.	+++	+++	++	+
3.	**Clear governance model for CIIP**: At the national level, CIP governance should not be complex. Only one or a few bodies should be involved, each with a clear assignment for sectoral coordination. Each critical infrastructure sector could have its own governance structure to monitor implementation of sector-specific CIP measures, and coordinate and strengthen collaboration among critical infrastructure owners and operators.	+++	+++	++	+
4.	**Dedicate a CIIP body**: A CIIP framework covers many critical aspects of national security and involves a broad number of sectors and stakeholders. Day-to-day operation and maintenance of CIIP requires dedicated attention and human and financial resources. Government should create an inter-agency body responsible for ensuring the resilience and protection of critical infrastructure from security threats. Many countries have found it practical to commission a CIIP dedicated agency for this work, while others created dedicated capabilities within existing institutions. The CIIP body should be responsible for policy oversight of national infrastructure in collaboration with industry, develop mechanisms to improve information sharing between the interconnected sectors, investigate vulnerabilities at critical infrastructures, and perform security audits. This body should strive to form CIIP competence and play a crucial role in the national CIIP framework.	+++	+++	++	+

(continued on next page)

TABLE 7.1. Consolidated List of Recommendations *(continued)*

		Clusters and relevance			
No.	**Recommendations**	**Stage 1**	**Stage 2**	**Stage 3**	**Stage 4**
5.	**Regulate:** Regulations should set standards for the security of critical infrastructure and requirements to restore and recover assets after emergency situations. Regulations should be addressed to critical infrastructure operators and design schemes to monitor particularly vulnerable critical infrastructure sites. An important objective of regulations is to require security incidents be reported to competent authorities (usually the national computer emergency response team). Instead of bans and restrictions, critical infrastructure operators should be helped to realize the benefits of including resilience thinking throughout their organizations and asset planning, from physical design to operational procedures and contingency planning. Lost revenues, reputational damage, contractual penalties, and the potential for litigation provide strong drivers for managing risks and building resilience.[a]	+	++	+++	+++
b. Critical Infrastructure Identification					
6.	**Define critical infrastructure:** Defining critical infrastructure is the very first step toward identifying critical infrastructures because it creates metrics. Most definitions include impact of disruption as one of the metrics. The extent of the impact is usually defined as nationwide. Another metric is the subject of disruption, which varies slightly from country to country. Security is one focus, however the traditional understanding of the security (as physical) needs to be broadened to include economic security.	+++	++	+	+
7.	**Assess risk:** Identification of critical infrastructures starts with a national-level risk assessment exercise. The aim of the exercise is to understand what risks are most likely to hinder national security, including economic security and citizen wellbeing. There are well-recognized risk assessment methodologies that can be used for this exercise.	++	++	+++	+++
8.	**Identify critical infrastructures:** After the risk assessment, risks need to be linked with the national infrastructures. Analysis should include understanding risk tolerance for each infrastructure asset and service. This will expedite selection of critical infrastructure sectors, subsectors, and assets within critical infrastructures. Those assets will compose the list of national critical infrastructures. Countries should clearly define which specific network assets are covered and should be secured and resilient. Countries that are starting to work on identifying critical infrastructures should adopt a methodology to identify critical assets and services as well as internal-external interdependencies. A step-by-step approach, starting with the identification of critical sectors, is recommended, followed by subsectors, services, and finally infrastructures and assets.	+++	+++	+	+
9.	**Database of identified critical infrastructure assets:** Information about all identified critical infrastructure assets should be stored in a centralized list. This information is usually classified. It is important to ensure that the national critical infrastructure list includes information about all critical infrastructure of national significance. Critical infrastructures that are identified at sub-national levels and that are not of strictly national standing could be listed within sub-national lists.	++	+++	++	++
10.	**List of critical infrastructure sectors**: Composition of the critical infrastructure sector list will vary from country to country depending on national circumstances. Six sectors were considered critical in all the reviewed countries and the EU: energy, transport, ICT, financial, water, and health. It is likely that these sectors will be considered critical in LAC countries as well.	+++	++	+	+
c. CIIP: Methods and Forms of Implementation					
11.	**Complementarity of efforts between public and private sectors**: CIIP policies should focus objectives and activities on supporting critical infrastructure operators in their efforts to protect operated assets as an alternative to substituting those efforts. This approach is considered more sustainable in the long term, as it eventually leads to the increased capacity for critical infrastructure operators and resilience of their assets. It also permits the reach of CIIP activities to be expanded and the efforts of each party to become complementary.	+++	+++	+++	+++

(continued on next page)

TABLE 7.1. Consolidated List of Recommendations *(continued)*

		Clusters and relevance			
No.	**Recommendations**	**Stage 1**	**Stage 2**	**Stage 3**	**Stage 4**
12.	**Partner with the private sector**: It takes time and effort to build the level of trust and cooperation needed for CIIP. It took 10 to 15 years for countries to put in place successful partnerships and deepen the level of cooperation. It will take time for developing countries since well-functioning partnerships involves comparable capacity and capabilities from both sides. The public sector will need to make an effort to be perceived as a strong partner in CIIP. Leveraging the national and regional academia for targeted CIIP research and development may be a good way to increase the capacity of the public sector in CIIP decision making and allow it to provide expertise and advice to the private sector.	+++	+++	+++	+++
13.	**Critical infrastructure operators:** Operators need to have a resilience strategy that uses the principles of redundancy, resistance, reliability, response, and recovery to protect against disruptions. This strategy requires buy-in from other stakeholders, including the supply chain, customers, and other operators. Because of growing physical and cyber security threats, critical infrastructure operators must implement incident management systems that cover systematic registration and investigation of, and reaction to, security incidents.	+	+	++	+++
14.	**Establish sectoral CIP working groups and develop community of CIP experts**: For all critical infrastructure sectors, in particular for those with high participation of private capital and a large number of actors (e.g., ICT, transport, and financial), it is advisable to establish CIP dedicated working groups or committees that would be led or co-led by the private sector. Those bodies would be instrumental in preparing and implementing national and sectoral CIP plans and they would enhance information exchange and build the CIP community. Regular CIP events at the national level as well as regular sectoral CIP gatherings to discuss current issues among the experts would raise the profile of the CIP agenda and identify where efforts should be strengthened. Through these structures, international cooperation and exchange of professional experience in CIP could be implemented.	+++	+++	++	+
15.	**Involve academia and the research community**: Assessments of the vulnerabilities and risks and other highly analytical work requires considerable research capacity that is usually not available within public institutions. Quality CIP plans cannot be built without scientific and technical foundation from national institutes and research centers. This approach should be considered in LAC as well since it could also be an opportunity to build collaboration between academia and the public sector. National standardization agencies could also be involved.	+++	+++	+++	+++
16.	**Skilled specialists and engineers:** Advanced skills are an important element of any CIP program. The issues related to CIP are relatively new, emerging, and sophisticated. To effectively implement a CIP framework, the public and private sectors need skilled specialists. Sometimes, the amount of funds invested into hardware and software is irrelevant, since it is up to specialists maintaining the critical infrastructure to use and implement those tools. Countries need to invest in training and building the capacity of existing critical infrastructure personnel. They should also encourage universities to develop science, technology, engineering, and mathematics study programs related to CIP and cyber security. Currently such programs are rare in academia.	+++	+++	+++	+++
d. Information Analysis and Sharing					
17.	**Bi-directionality of information sharing**: Good information sharing is a bi-directional, PPP-type of activity, meaning it involves the public and private sectors. It is also requires a continuous effort to maintain strong relationships with information sharing partners.	+++	+++	+++	+++
18.	**Trust and face-to-face communication**: Experts in the best practices of information sharing emphasize that quality exchanges cannot be achieved without a high level of trust.[b] Any electronic system dedicated to information sharing could not build that trust and should not replace good interpersonal relationships achieved through regular face-to-face meetings.	+++	+++	++	++

(continued on next page)

TABLE 7.1. Consolidated List of Recommendations *(continued)*

		Clusters and relevance			
No.	**Recommendations**	**Stage 1**	**Stage 2**	**Stage 3**	**Stage 4**
19.	**Use electronic tools to share CIIP information**: When trust and relationships are maintained, well-functioning electronic systems provide good facilitation of the process and make it more efficient. In particular, electronic systems are effective in cases of big CIP communities, like the EU and the United States. Though electronic systems can facilitate information exchange, it is important to understand that they are not essential to the information sharing process.	+	+	++	+++
20.	**Early warning system**: Any early warning system is a practical and useful CIP prevention tool. The purpose of such systems is to detect security threats and cyber-attacks, identify critical infrastructure vulnerabilities, prepare for the danger, and act accordingly to mitigate or avoid it. All countries should invest in an early warning system at the national and cross-sectoral levels.	+	++	+++	+++
21.	**Mandate information sharing**: Practical collaboration in information sharing has proven that, first and foremost, it should be promoted as a voluntary process and that obligations usually have limited success. Legal tools mandating information sharing should be enacted to a limited degree and for well-defined purposes, as in the case of risk assessments and incident reporting. Mandatory incident reporting of large disruptions is mandated in the EU. In regards to highly confidential information that necessitates sharing, it must be regulated and captured by the relevant legal frameworks as the nature of the information tends to be sensitive from both the commercial and security standpoints.	+++	+++	++	+
e. Crisis Management Practices					
22.	**Assess national risks and national CIP plan**: Regular assessment of national risks supports the shaping of national strategic priorities, and CIP measures and priorities. While performing national risk assessment, countries are increasingly going beyond the risks that arise domestically to include the international context. Different countries find themselves susceptible to different sets of risks than the others, since there is no one-size-fits-all archetype. National risk assessment should lead to preparing a national CIP plan that would aim to address and mitigate those risks. Such a plan should provide clear guidance and designate responsibilities for how security and reliability of the national assets are ensured, coordinate public–private initiatives, and put in place implementation review processes.	+++	+++	++	+
23.	**Regularly assess critical infrastructure and prepare sectoral CIIP plans**: Routine assessment of the resilience of each critical infrastructure sector to identify risks is a good practice as it monitors the state of critical infrastructure assets, enabling gradual enhancements and adjustments for increased resilience. The latter process could be integrated within sectoral CIP plans. Agencies should be assigned to lead CIP efforts at the sector level and critical infrastructure operators that fully or partially operate identified critical infrastructure. Sectors need to enforce more **frequent inspection of critical infrastructure** and update the list of critical assets. Due to rapid advancements in the interconnection of systems, a system component previously assessed as non-critical can become critical in a short time.	++	+++	+++	+++
24.	**Manage security incidents:** Incident management is one of key elements of CIP. Security incidents should be reported, investigated, and reacted to in a timely manner through efficient Security Incidents Management. As cyber-attacks impact not only the ICT sector, but are threats to all critical infrastructures, systematically adopting computer emergency response activities from a national level team to sectoral teams for critical infrastructure operator networks is recommended. This would improve security events detection, reaction and execution.	++	+++	+++	+++
25.	**Exercise**: Simulated exercises are tools to understand and increase critical infrastructure preparedness, detection of possible gaps in security, and resilience. These exercises also support relationships and partnerships within the critical infrastructure community. Performing regular exercises at the national and sector levels as well as between interconnected sectors is recommended.	+	+++	+++	+++

[a] Peter Guthrie, Thalia Konaris, 2012. Infrastructure Resilience, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/286993/12–1310-infrastructure-and-resilience.pdf.

[b] Ibid.

References

Alberti, J. 2015. "Pre-Investment in Infrastructure in Latin America and the Caribbean: Case Studies from Chile, Mexico, Peru, and Uruguay." Monograph Series No. IDB-MG-286. Washington, DC: Inter-American Development Bank. Available at http://publications.iadb.org/bitstream/handle/11319/6792/Pre-Investment-Infrastructure.pdf?sequence=1.

Arsht, A. 2014. "Urbanization in Latin America." Washington, DC: Atlantic Council. Available at http://www.atlanticcouncil.org/publications/articles/urbanization-in-latin-america.

Atkins. 2015. "The Skills Deficit: Consequences & Opportunities for UK Infrastructure." China: Atkins. Available at http://www.atkinsglobal.com/~/media/Files/A/Atkins-Corporate/uk-and-europe/uk-thought-leadership/reports/The%20Skills%20Deficit%20Report%20for%20Digital%20Infrastructure.pdf.

Baker, S., N. Filipiak, and K. Timlin. 2011. "In the Dark: Crucial Industries Confront Cyberattacks." McAfee Second Annual Critical Infrastructure Protection Report. Written with the Center for Strategic and International Studies (CSIS). Santa Clara, CA: McAffee. Available at http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf.

Buldyrev, S. V., et al. 2010. "Catastrophic Cascade of Failures in Interdependent Networks." *Nature*. 464(7291): 1025–28. Available at www.nature.com/nature/journal/v464/n7291/full/nature08932.html.

Calderón, C., and L. Servén. 2010. "Infrastructure in Latin America." Policy Research Working Paper 5317. Washington, DC: The World Bank. Available at https://openknowledge.worldbank.org/bitstream/handle/10986/3801/WPS5317.pdf.

Choi, D. S., K. H. Yoon, and J. D. Shin. 2014. "A Study on Law Analysis for Efficient Critical Infrastructure Protection." *Journal of the Korean Society of Hazard Mitigation*. 14(1): 223–45. Available at http://scholar.ndsl.kr/schArticleDetail.do?cn=JAKO201412835899931.

CPNI (Center for the Protection of National Infrastructure). 2010. "Protection against Terrorism, 3rd Edition." London, UK: CPNI. Available at http://www.cpni.gov.uk/documents/publications/2010/2010002-protecting_against_terrorism_3rd_edition.pdf?epslanguage=en-gb.

DHS (Department of Homeland Security). 2003a. "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets." Washington, DC: DHS, Government of the United States of America. Available at https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

_____ . 2003b. "The National Strategy to Secure Cyberspace." Washington, DC: Department of Homeland Security, Government of the United States of America. Available at https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

———. 2007. “National Strategy for Homeland Security.” Washington, DC: Department of Homeland Security, Government of the United States of America. Available at http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf.

———. 2013a. “Executive Order 13636: Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive 21: Critical Infrastructure Security and Resilience.” Fact Sheet. Washington, DC: Department of Homeland Security, Government of the United States of America. Available at http://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf.

———. 2013b. “NIPP 2013: Partnering for Critical Infrastructure Security and Resilience.” Washington, DC: Department of Homeland Security, Government of the United States of America. Available at http://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf.

———. 2014a. “Protected Critical Infrastructure Information Program.” Fact Sheet. Washington, DC: Department of Homeland Security, Government of the United States of America. Available at https://www.dhs.gov/sites/default/files/publications/PCII-Fact-Sheet-2014-508.pdf.

Dobbs, R., J. Manyika, and J. Woetzel. 2015. “The Four Global Forces Breaking All the Trends.” McKinsey Global Institute. Available at http://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/the-four-global-forces-breaking-all-the-trends.

Dobbs, R., S. Smit, J. Remes, J. Manyika, C. Roxburgh, and A. Restrepo. 2011. “Urban World: Mapping the Economic Power of Cities.” McKinsey Global Institute. Available at http://www.mckinsey.com/~/media/McKinsey/Global%20Themes/Urbanization/Urban%20world/MGI_urban_world_mapping_economic_power_of_cities_full_report.ashx.

EC (European Commission). 2004. “Critical Infrastructure Protection in the Fight against Terrorism.” Communication from the Commission to the Council and the European Parliament, COM(2004) 702 final. Commission of the European Communities. Brussels: EC. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0702&from=EN.

———. 2006. “A European Programme for Critical Infrastructure Protection.” Communication from the Commission, COM(2006) 786 final. Commission of the European Communities. Brussels: European Commission. Available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786.

———. 2010a. “The EU Internal Security Strategy in Action: Five Steps Towards a More Secure Europe.” Communication from the Commission to the European Parliament and the Council, COM(2010) 673 final. Commission of the European Communities. Brussels: European Commission. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0673&from=EN.

———. 2010b. “The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens.” Notices from European Union Institutions, Bodies, Offices and Agencies. *Official Journal of the European Union*. 115:1–38. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010XG0504(01)&from=EN.

———. 2011. “Recommended Elements of Critical Infrastructure Protection for Policy Makers in Europe: Good Practices Manual for CIP Policies.” Brussels: Directorate-General Home Affairs, European Commission. Available at http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/FINAL_RECIPE_manual.pdf.

———. 2012a. “The Review of the European Programme for Critical Infrastructure Protection (EPCIP).” Commission Staff Working Document, SWD(2012) 190 final. Commission of the European Communities. Brussels: European Commission. Available at http://ec.europa.eu/dgs/home-affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf.

——— . 2012b. “Position Paper on EU Policy on Critical Energy Infrastructure Protection.” Brussels: European Commission. Available at http://ec.europa.eu/energy/sites/ener/files/documents/20121114_tnceip_eupolicy_position_paper.pdf.

———. 2013. “A New Approach to the European Programme for Critical Infrastructure Protection, Making European Critical Infrastructure More Secure.” Commission Staff Working Document, SWD(2013) 318 final. Commission of the European Communities. Brussels: European Commission. Available at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf.

ENISA (European Union Agency for Network and Information Security). 2015. “Methodologies for the Identification of Critical Information Infrastructure Assets and Services.” Heraklion, Greece: ENISA. Available at https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis.

Espinosa, E. I. 2015. “Hacia una estrategia nacional de ciberseguridad en México.” *Journal of Public Administration*, National Institute of Public Administration (INAP), Mexico, 136, January to April. Available at https://www.academia.edu/12107238/Towards_a_Cybersecurity_Strategy_in_Mexico.

EU (European Union). 2003. “A Secure Europe in a Better World.” European Security Strategy of the European Council. Brussels: EU. Available at http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf.

———. 2008. “The Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection.” Council Directive 2008/114/EC. *Official Journal of the European Union*. 345:75–82. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114.

fDi Intelligence. 2014. “The fDi REPORT 2014: Global Greenfield Investment Trends.” London, UK: The Financial Times Ltd. Available at http://ftbsites.ft.com/forms/fDi/report2014/files/The_fDi_Report_2014.pdf.

———. 2015. “The fDi REPORT 2015: Global Greenfield Investment Trends.” London, UK: The Financial Times Ltd. Available at http://report.fdiintelligence.com/.

Figueroa, V., D. L. Vera, and L. Hormazábal. 2011. “Chilean Armed Forces and their Role in Emergencies, Disasters and Catastrophes: Considerations for an Institutional Policy on Psychosocial Education.” Santiago: Pontificia Universidad Catolica De Chile, Facultad De Medicina, Departamento de Psiquiatría. Available at http://medicina.uc.cl/docman/cat-view/1380.

Finland. 2004. “Finnish Security and Defence Policy 2004.” Helsinki: Prime Minister’s Office, Government of Finland. Available at http://www.defmin.fi/en/publications/finnish_security_and_defence_policy.

———. 2006a. “The Strategy for Securing the Functions Vital to Society.” Government Resolution 23.11.2006. Helsinki: The Security and Defense Committee, Government of Finland. Available at http://www.defmin.fi/files/858/06_12_12_YETTS__in_english.pdf.

——— . 2006b. “A Renewing, Human-Centric and Competitive Finland: The National Knowledge Society Strategy 2007–2015.” Helsinki: Information Society Programme, Prime Minister’s Office, Government of Finland. Available at http://www.umic.pt/images/stories/publicacoes1/Strategia_englanti_181006final.pdf.

——— . 2011. “Security Strategy for Society.” Government Resolution 16.12.2010. Helsinki: Ministry of Defence, Government of Finland. Available at http://www.defmin.fi/en/topical/press_releases/2011/the_security_strategy_for_society_now_available_for_download_in_english.4724.news.

——— . 2013. “Finland’s Cyber Security Strategy.” Finland Government Resolution 24.1.2013. Helsinki: Secretariat of the Security Committee, Government of Finland. Available at http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

Finnish Technology Industries. 2014. “Economic Situation and Outlook.” Helsinki: The Federation of Finnish Technology Industries. Available at http://teknologiateollisuus.fi/en/news/situation-and-outlook-finnish-technology-industry-12014.

Germany. 2009. “National Strategy for Critical Infrastructure Protection (CIP Strategy.” Bonn: Federal Ministry of the Interior, Federal Republic of Germany. Available at http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf.

Giannopoulos, G., R. Filippini, and M. Schimmer. 2012. “Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art.” JRC Technical Note EUR 25286 EN – 2012. Brussels: Joint Research Center-Institute for the Protection and Security of the Citizen, European Commission. Available at: http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf.

Guthrie, P., and T. Konaris. 2012. “Infrastructure and Resilience.” Foresight project ‘Reducing Risks of Future Disasters: Priorities for Decision Makers’. Report produced for the Government Office of Science. London, UK: Government of the UK. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/286993/12-1310-infrastructure-and-resilience.pdf.

Hämmerli, B., and A. Renda. 2010. “Protecting Critical Infrastructure in the EU.” Brussels: Centre for European Policy Studies. Available at http://aei.pitt.edu/15445/1/Critical_Infrastructure_Protection_Final_A4.pdf.

ICE (Institution of Civil Engineers). 2009. “The State of the Nation: Defending Critical Infrastructure.” London, UK: ICE. Available at https://www.ice.org.uk/getattachment/media-and-policy/policy/state-of-the-nation-critical-infrastructure-2009/SoN_DCIreport_final_web.pdf.aspx.

ISO (International Organization for Standardization). 2013. “Information Technology – Security Techniques – Information Security Management Guidelines Based on ISO/IEC 27002 for Process Control Systems Specific to the Energy Utility Industry.” ISO/IEC TR 27019:2013. Geneva: ISO. Available at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43759.

ITU (International Telecommunication Union). 2008. “Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts.” ITU Study Group Q.22/1. Geneva: ITU. Available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf.

Jefatura del Estado. 2011. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Available at http://www.sisonline.com/files/7387.pdf

Jonkeren, O. E., et al. 2012. “Economic Impact Assessment of Critical Infrastructure Failure in the EU: A Combined Systems Engineering – Inoperability Input-Output Model.” The 20th International Input-Output Conference. Available at https://www.iioa.org/conferences/20th/papers/files/903_20120516091_JonkerenIIOA2012SE-IIMmodel.pdf.

Korea. 2010. “Framework Act on the Management of Disasters and Safety.” Korea Act No.10347. Sejong-si: Reliable Ministry of Government Administration, Republic of Korea. Available at http://www.law.go.kr/eng/engMain.do.

———. 2013. “Act on the Protection of Information and Communications Infrastructure.” Act No. 11690. Seoul: Government of Korea. Available at http://www.law.go.kr/engLsSc.do?menuId=0&subMenu=5&query=%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EA%B8%B0%EB%B0%98%EB%B3%B4%ED%98%B8%EB%B2%95#liBgcolor0.

———. 2015. “Enforcement Decree of the Framework Act on the Management of Disasters and Safety.” Korea Presidential Decree No. 26285. Seoul: Government of Korea. Available at http://www.law.go.kr/engLsSc.do?menuId=0&subMenu=5&query=%EC%

9E%AC%EB%82%9C%20%EB%B0%8F%20%EC%95%88%EC%A0%84%20-%20liBgcolor4#liBgcolor0.

Microsoft. 2014. "Microsoft Security Intelligence Report, Volume 17." Redmond, US: Microsoft. Available at http://www.microsoft.com/en-us/download/confirmation.aspx?id=44937.

Min, H-S J., et al. 2009. "Toward Modeling and Simulation of Critical National Infrastructure Interdependencies." Washington, DC: National Infrastructure Simulation and Analysis Center (NISAC), Department of Homeland Security, Government of the United States of America. Available at http://www.sandia.gov/nisac/wp/wp-content/uploads/downloads/2012/04/modeling-and-simulation-of-critical-infrastructure.pdf.

Ministerio del Interior. 2011. "Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas." Available at http://www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf.

OECD (Organisation of Economic Co-operation and Development). 2008. "Malicious Software (Malware): A Security Threat to the Internet Economy." Ministerial Background Report, DSTI/ICCP/REG(2007)5/FINAL. Paris: OECD. Available at http://www.oecd.org/dataoecd/53/34/40724457.pdf.

Pitt, M. 2008. "Learning Lessons from the 2007 Floods." Available at http://webarchive.nationalarchives.gov.uk/20100807034701/http:/archive.cabinetoffice.gov.uk/pittreview/_/media/assets/www.cabinetoffice.gov.uk/flooding_review/pitt_review_full%20pdf.pdf.

Richardson, J. P. 2008. "A Management Framework for Organizing National Cybersecurity/CIIP Efforts." ITU-D Secretariat. Geneva: International Telecommunication Union. Available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/richardson-cybersecurity-framework-and-readiness-assessment-CITEL-Mar-08.pdf.

Schmitt, M. N. 2013. "Tallinn Manual on the International Law Applicable to Cyber Warfare." Prepared for the NATO Cooperative Cyber Defense Center of Excellence. Cambridge: Cambridge University Press. Available at https://issuu.com/nato_ccd_coe/docs/tallinnmanual/3?e=0/1803379.

Spain. 2007. *"Acuerdo sobre protección de infraestructuras críticas."* Madrid: Ministry of Interior, Government of Spain. Available at http://www.cnpic.es/Biblioteca/Legislacion/Generico/ACUERDO_CONSEJO_DE_MINISTROS_de_2_de_noviembre_de_2007.pdf.

———. 2013a. "The National Security Strategy: Sharing a Common Project." Madrid: Prime Minter's Office, Government of Spain. Available at http://www.lamoncloa.gob.es/documents/estrategiaseguridad_baja_julio.pdf.

———. 2013b. "National Cyber Security: Strategy 2013." Madrid: Prime Minter's Office, Government of Spain. Available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf.

Theodore Puskas Foundation. 2013. *CIIP Matters*. 7(1). Available at http://www.cnpic.es/Biblioteca/Noticias/Newsletter_Meridian_vol7_no1_June_2013.pdf.

UK (United Kingdom). 2007. "A National Information Assurance Strategy." London, UK: Central Sponsor for Information Assurance, Cabinet Office, Government of the UK. Available at http://old.culture.gov.uk/images/working_with_us/nia_strategy.pdf.

———. 2010a. "Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards." London: Cabinet Office, Government of the United Kingdom. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf.

———. 2010b. "A Strong Britain in an Age of Uncertainty: The National Security Strategy". London, UK: Cabinet Office, National Security and Intelligence, Government of the United Kingdom. Available at https://www.gov.uk/government/uploads/system/uploads/

attachment_data/file/61936/national-security-strategy.pdf.

———. 2011. "Keeping the Country Running: Natural Hazards and Infrastructure: A Guide to Improving the Resilience of Critical Infrastructure and Essential Services." London: Cabinet Office, Government of the United Kingdom. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61342/natural-hazards-infrastructure.pdf.

———. 2013a. "A Summary of the 2013 Sector Resilience Plans." London: Cabinet Office, Government of the United Kingdom. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/271370/SRP_Public_Summary_2013.pdf.

———. 2013b. "Government Launches Information Sharing Partnership on Cyber Security." Press Release. London: Cabinet Office, Government of the United Kingdom, and The Rt Hon Lord Maude of Horsham. Available at https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security.

———. 2015. "2010 to 2015 Government Policy: Cyber Security." Policy Paper. London: Cabinet Office, Government of the United Kingdom. Available at https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security.

UNAM (National Autonomous University of Mexico). 2015. "Artículo 28 Constitución Política de los Estados Unidos Mexicanos." Instituto de Investigaciones Jurídicas. Mexico City, Mexico: UNAM. Available at http://info4.juridicas.unam.mx/ijure/fed/9/29.htm?s.

U.S. White House. 1998. "Critical Infrastructure Protection." Presidential Decision Directive/NSC-63. Washington, DC: White House, Government of the United States of America. Available at http://fas.org/irp/offdocs/pdd/pdd-63.htm.

———. 2003. "Critical Infrastructure Identification, Prioritization, and Protection." Homeland Security Presidential Directive/Hspd-7. Washington, DC: White House, Government of the United States of America. Available at http://georgewbush-whitehouse.archives.gov/news/releases/2003/12/20031217-5.html.

———. 2013. "Critical Infrastructure Security and Resilience." Presidential Policy Directive/ PPD-21. Washington, DC: White House, Government of the United States of America. Available at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

WEF (World Economic Forum). 2012. "Strategic Infrastructure: Steps to Prioritize and Deliver Infrastructure Effectively and Efficiently." Geneva: WEF. Available at http://www3.weforum.org/docs/WEF_IU_StrategicInfrastructure_Report_2012.pdf.

———. 2015. "Global Risks 2015, 10th Edition." Geneva: World Economic Forum. Available at http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf.

World Bank. 2014. "World Development Report 2014: Risk and Opportunity: Managing Risk for Development." Washington, DC: The World Bank. Available at http://siteresources.worldbank.org/EXTNWDR2013/Resources/8258024-1352909193861/8936935-1356011448215/8986901-1380046989056/WDR-2014_Complete_Report.pdf.

———. 2016. "The World Bank Group A to Z 2016“. Washington, DC: World Bank. Abailable at https://openknowledge.worldbank.org/handle/10986/22548

ZAGREB. 2008. "*Informe Final: Estudio para la definición e identificación de infraestructura crítica de la información en Chile*." ZAGREB Consultores Limitada. Available at http://www.subtel.gob.cl/images/stories/articles/subtel/asocfile/infraestructura_critica_020309_v1.pdf.

KISA

IDB