Chapter 1
Critical Infrastructures, Protection and Resilience

Roberto Setola, Eric Luiijf and Marianthi Theocharidou

Abstract This chapter introduces the concept of Critical Infrastructure (CI). Although old civilisations had CI, the protection and resilience of CI has come to the fore again in the last two decades. The risk to society due to inadvertent and deliberate CI disruptions has largely increased due to interrelation, complexity, and dependencies of these infrastructures. The increased use of information and telecommunication technologies (ICT) to support, monitor, and control CI functionalities has contributed to this. The interest in CI and complex systems is strongly related to initiatives by several governments that from the end of the 90s of the previous century recognised the relevance of the undisturbed functioning of CI for the wellbeing of their population, economy, and so on. Their policies highlighted early the increasing complexity of CI and the challenges of providing such CI services without disruption, especially when accidental or malicious events occur. In recent years, most national policies have evolved following a direction from protection towards resilience. The need for this shift in perspective and these concepts are also analysed in this chapter.

1 Introduction

Old civilisations like the Romans already protected their Critical Infrastructure (CI) such as aqueducts and the military roads. More recently, nations planned for the protection of their key infrastructure elements such as power plants, bridges and

R. Setola (✉)
Università Campus Bio-Medico, Rome, Italy
e-mail: r.setola@unicampus.it

E. Luiijf
Netherlands Organisation for Applied Scientific Research TNO, The Hague, The Netherlands
e-mail: eric.luiijf@tno.nl

M. Theocharidou
European Commission, Joint Research Centre, Ispra, Italy
e-mail: marianthi.theocharidou@jrc.ec.europa.eu

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*,
Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_1

harbours in the cold war era. In the relatively quiet 80s of the previous century the protection efforts of these key points seemed to be less prominently needed. At the same time, the risk to the society due to inadvertent and deliberate CI disruptions gradually increased considerably. A number of colliding factors reinforcing the recent CI-related risk increases:

(1) the diminishing governmental control due to liberalisation and privatisation of infrastructures,
(2) the increased use of information and telecommunication technologies (ICT) to support, monitor, and control CI functionalities,
(3) the idea of the population that services can and, above all, shall be available 24/7,
(4) urbanisation which stresses the utilisation of old infrastructures to their limits,
(5) the increasing interwovenness, (supply) chaining and dependencies of infrastructural services,
(6) adversaries of the society who increasingly understand that a successful attack may create havoc.

Several of these trends and their related risk to the society were recognised by the Clinton Administration in the 90s. In response, the US Presidential Decision Directive PDD-63 [1] set forth a set of actions in 1998. The PDD-63 defined CI as "*those physical and cyber-based systems essential to the minimum operations of the economy and government*". Triggered by the PDD-63 and the millennium bug (Y2K), some other nations (e.g. Canada) started their CI studies and protection activities. In February 2001, Canada started its Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) within the Department of National Defence organisational structure [2]. The 11/9 event triggered more nations to put CI and their protection high on the list of their activities as the long forgotten cold war infrastructure protection plans looked outdated and ineffective [3].

While there is not a commonly accepted definition of critical infrastructure (CI), all definitions emphasise the contributing role of a CI to the society or the debilitating effect in the case of disruption [4]. On 17 November 2005, the European Commission adopted a Green Paper on a European Programme for Critical Infrastructure Protection [5]. In 2008, the European Council issued the Directive 2008/114/EC [6], which required the Member States to identify and designate European CI (ECI) and assess the needs for their protection. This Directive defined 'critical infrastructure' as:

> An asset, system or part thereof located in Member States which 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 in a Member State as a result of the failure to maintain those functions [6].

This directive referred to infrastructures of European dimension, but it triggered several Member States to identify their national CI (NCI) as well. Currently, one can find many more nations who use an equivalent of this definition without the "in a Member State" parts (see e.g. [4]). However, despite this common definition, an

open question remains: "what exactly comprises CI?". First of all, nations may define critical sectors, e.g. telecommunications, energy, transportation, drinking water, and more. Secondly, nations may define critical functions or services of these sectors (e.g. the production of isotopes for cancer treatments). Looking deeper, one may identify which components, parts, and subsystems have to be really considered as a "critical" to the critical functions of critical sectors.

Moreover, it shall be noted that the European definition not only applies to 'technical' infrastructures but also to societal and soft infrastructures.

The directive also defined the notion Critical Infrastructure Protection in an **all-hazard** perspective: "all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability" [6].

2 Importance of Protection and Resilience

However, the most interesting question is why we need to increase our interest about the protection and resilience of such systems. The answer to this question can be found still in the PDD-63 that about 20 years ago stated:

> Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks" [1].

Indeed as outlined above as well as noted in [7], many economic, social, political and technological reasons have caused a rapid change in the organisational, operational and technical aspects of infrastructures. These infrastructures, that in the past could be considered as autonomous vertically integrated systems with very few points of contact with respect to other infrastructures, are now tightly coupled and show large numbers of dependencies. This has generated many positive effects to our society and the well-being of populations, but has increased the complexity, the vulnerability of infrastructures and the related risk to our societies at the same time.

Several episodes emphasised such fragility. TNO has collected more than 9,550 CI disruption events which caused the failure of 12,400 infrastructure services through cascading between 2005 and now. Some example events are described in Table 1.

Even if the example incidents illustrated in Table 1 are very different in terms of primary causes, extension and consequences, all of them are characterised by non-intuitive dependencies and, especially, by inadequate protection measures to manage the crisis. This is mainly due to the incomplete understanding of an event and especially of its direct and indirect consequences [8, 9]. This is, unfortunately, an effect of the increased complexity of the socio-technical scenario largely characterised by the presence of dependencies among different CI.

Table 1 Some example incidents of CI disruptions

1998
On May 19, 1998, the telecommunication satellite Galaxy IV spun out of control. That produced many unexpected problems in North America for several days before another replacement satellite could take over the services: about 40 million of pagers out-of-services causing major problems to dispatch doctors and nurses in hospitals and to notify first responders fast. CBS, ABC, CNN and other media networks lost nation-wide transmission signals. Air transportation was affected due to absence of high-altitude weather reports; 30 flights from Huston airport were cancelled or delayed. At the highway: drivers could not perform refuel because gas-stations lost the capability to process credit cards.
2001
On July 18, 2001, train wagons containing chloride acid derailed in a downtown tunnel in Baltimore. Fire fighters, in the absence of information about the presence of chloride acid on the train, decided to let the train burn. Unknown was also that a high-pressure water mains, a set of glass fibres and a power transmission cable were located just up the same tunnel. Due to the fire, the water transport pipeline to downtown burst open. As a result over 70 million gallons of water flooded downtown streets and houses; the drinking water supply failed, and the fire fighters lost their water supply. Glass fibres melted and caused a noticeable world-wide slowdown on the internet and caused local and international telephony outages. Over 1200 buildings lost power.
2001
The collapse of Twin-towers due to the "9/11 events" caused the inoperability of many infrastructures (electricity, water, gas, communication, steam distribution, metro, operations of key financial institutions) in a broad area of Manhattan. Moreover, the presence in that area of important telco-nodes induced degradation in telecommunication and on Internet also outside US. This large impact has been caused by the co-location of a multitude of vital CI inside the World Trade Centre. Indeed in those building there were the Port Authority Emergency Management centre, the Office of Emergency Management Operations Center, electrical power substations, steam and gas distribution, metro stations, further to be the headquarters of a number of financial institutions. Moreover also the emergency operations were affected by such extreme co-location For instance, the Verizon building 140 West St., contained 306,000 telephony and over 55,000 data lines from 30 operators and provided services to 34,000 customers in Lower Manhattan. A set of these lines was connected to antennas for first responders and mobile telephony at the roof of the towers and adjacent buildings. The communication capacity for the first responders was almost immediately lost due the fire and subsequent collapse of the WTC towers. Data and telephony services failed as the Verizon building became damaged by falling debris. Lines were cut and backup power was lost due to the flooding of batteries. Many of the communication back-up lines for first responders and agencies involved in disaster management were co-located with the primary circuits and failed. The remaining fixed and wireless communication for emergency response failed as police did not allow Verizon to refill the fuel tanks for their back-up power generators at two other, still operating, communication switch locations. During the recovery phase, police did not allow crews of all co-located operators to enter the closed-off area; only crews of Verizon were allowed to work on repairs. Verizon T-shirts allowed repair crews of AT&T and other telecommunication companies to enter the area and perform their work.
2004
In the area on Rome (Italy) during the night of 31st December there was a problem at the air-conditioning system of an important telecommunication node. The problem had not been adequately managed causing an increased degradation up to the complete collapse of the node. The telecommunication operator had no elements (neither information) to foresee which services

(continued)

Table 1 (continued)

would be impacted by the failure. They decided to not provide any warning while trying to solve the problem internally. Unfortunately they were unable to manage the situation. The direct consequence was the stop for some 6 h of all wired and mobile telephone communication in large area of Rome. Moreover as an indirect consequence, more than 5000 bank and 3000 postal offices nationwide were without communications. Moreover, 70% of check-in desks at Rome airport were inoperable (with delays for several flights). Finally they were close to an electric blackout because the electric distribution system operators abruptly lost the ability to supervise and manage of half of Rome's power grid.
2010
Mid April 2010, the Eyjafjallajoekull volcano on Island erupts through fast cooling ice cap (a so-called VEI 4 class eruption). As a result glass particles are blown into air and transported to Europe in several waves during a month. Depending on the jet stream, some 30 European nations from Sweden to Turkey had to close down their airspace affecting hundred thousands of passengers. Just-in-time transport by plane, e.g. of repair parts, as well as medicines and donor organs for transplantation could not take place. The financial loss for the tourist sector was 1 billion euro. The air transport industry lost 1.5–2.5 billion euro. The worldwide GDP impact was 5 billion US dollar.
2016
On January 4, 2016, a special weather condition caused a layer of five centimetre of black ice in the northern part of The Netherlands which impacted various CI for several days. High voltage lines develop a "wing profile" causing dangling of the lines with power dips as a result. Hospitals regard the risk of power outages too high and stopped all non-life threatening surgeries. Schools are closed. Road and rail transport was not possible to a large extent. Milk collection at farms was halted. Milk products cannot be produced anymore and distributed to supermarkets across a larger part of the Netherlands. Schools were closed for days. The air force cannot scramble their F16s anymore.

Indeed, as emphasised by the different studies performed on the emergency response after 9/11, during such a crisis there was not a clear understanding of the CI dependencies, and the need for CI protection. Moreover, the New York City emergency preparedness plans did not account for total neighbourhood and facility disasters. The emergency plans and back-up tapes with databases were inaccessible as they were in the NY city hall which was powerless and inaccessible as a result of the collapse of the two World Trade Center (WTC) towers. The Emergency Operations Center at WTC 7 was destroyed and had to be relocated three times during the emergency operations, something the operation plans did not prepare for. Finally emergency plans developed by CI operators and financial institutions did take into account the possibility of multiple CI failure, all of them considered a scenario where only their CI collapsed (see e.g. [10, 11]).

These events show that a more careful understanding of the set of CI, their dependencies and common cause failure risk along with their full operational conditions is needed. A first step is to revisit analysis reports of earlier disasters/emergencies to know the possible causes. Moreover, one can learn from the potential consequences and of decisions taken by crisis response organisations without of a clear understanding of the relationship between the different CI

services, CI elements, and actors (e.g. crisis management, CI operators). Such an analysis will stress the relevance to have a good knowledge of all the infrastructures and the services they provide, their element which operate (or are located) in a given area, and of their dependencies. This means that one has to have at least information about the geographical location of the most relevant components of the different infrastructures, as well as their function within the whole infrastructure, and possible single points of failure (also known as "key points"). Organisationally one needs to have points of contact within each of the actor organisations as "one shall not exchange business cards during an emergency".

There is the need to have methodologies and tools to support the analysis of such complex (critical) systems with earlier events as a starter. Indeed we have to consider several elements that may reduce the effectiveness of analysis performed exclusively on historical data. This is partly due to the increasing diffusion of ICT technologies, which changes significantly the operational modes of the different infrastructures. Another aspect is that high impact, low frequency events may occur that seldom that the analysis of recent events may overlook important CI dependency aspects. This effect may be amplified by the fact that near missies in CI disruptions are not reported and analysed outside the CI operator's organisation, if at all.

We also need to consider scenarios where several CI may be affects by a common mode failure event so as to take into account the operative condition of the different CI. Moreover, the relevance and impact of dependencies may largely be influenced by the actual operative conditions [12].

All these aspects call for the availability of sophisticated analysis and simulation tools, as illustrated in the next chapters of this book, while this chapter provides an overview of a selection of relevant initiatives that are on-going in the sector of CI protection and resilience.

3 Government Initiatives: Policies and Research

In this section we highlight a selection of international policies in order to identify their focus and priorities with respect to CI and CIP.

The governments of different nations recognise the increasing importance of CI protection and resilience. This is demonstrated by the policies they implement with respect to CI at sectorial and cross-sectorial levels. In parallel, these policies are frequently followed by funding to universities, national laboratories, and private companies involved in the modelling, simulation and analysis (MS&A) of CI dependencies (e.g. see [13]), which have further led to much innovative and diverse work [14].

Overall, several nations have put in place a policy for critical infrastructure protection (CIP) and also for critical information infrastructure protection (CIIP). In the recent years, we also observe a shift of the focus from CIP towards

infrastructure 'resilience',[1] even if the two concepts are not easily distinguished. The landscape of these national policies remains still very fragmented.

Moreover, government and international institutions recognised that to manage the complexity of the problem at hand there is the need to develop new methodologies, paradigms and tools. To this end several programs have been set up. Several scientific programs and institutions have been established in order to protect and strengthen CI [14]. These initiatives include, among others, the US National Infrastructure Simulation and Analysis Center (NISAC), the European Reference Network for Critical Infrastructure Protection (ERNCIP), the Critical Infrastructure Program for Modeling and Analysis (CIPMA) in Australia, the National Critical Infrastructure Assurance Program (NCIAP) in Canada, the Dutch Approach on Critical Infrastructure Protection in the Netherlands, the Critical Infrastructure Resilience Program in the UK, and the Critical Infrastructure Protection Implementation Plan in Germany. These initiatives provide a progress in the knowledge of the problems at hand so as on the possible solutions. It is interesting to note that up to 2008 the majority of R&D projects were related to security at component level [13]. Some projects focused on strategic national oriented aspects, and only few addressed problems induced by dependencies of infrastructures. The presence of such R&D programs gave rise to the methodological and technological instruments to manage the complexity emerging from dependencies among CI allowing to provide some operational tools to stakeholders, decision makers and policy makers.

3.1 The US Approach

As described above, the increased relevance of CI was recognised in the US in the mid 90s. In 1998, the Presidential Policy Directive No. 63 [1] on Critical Infrastructure Protection (CIP) recognised the need to address vulnerabilities of CI and the need for flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security. A detailed overview of how the CIP policy has developed in the US is presented in [17].

Currently, according to Presidential Policy Directive/PPD-21, "it is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats" [18]. CI is defined by the USA PATRIOT Act[2] as:

[1]While there are no established European Union definitions of 'resilience' in the CI context, one can still find several non-official and more official definitions of the concept [15]. A suitable generic definition, applicable also for CI, is provided by UNISDR [16]: "The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions" [16].

[2]§1016(e) of the United States Patriot Act of 2001 (42 U.S.C. §5195c(e)).

> Systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters.

As explained in [17], the US federal government works with states, local authorities, and the owners and operators of CI (in both the private and public sector) to identify those specific assets and systems that constitute the nation's CI. Together, these entities perform a risk management approach for these assets, in order to assess vulnerabilities to the threats facing the nation, assess risk, and identify and prioritise a set of measures that can be taken to mitigate risk. The approach is a voluntary one, with primary responsibility for action lying with the owners and operators of CI. The federal government, however, will intervene in case of inadequate protection or response.

According to Moteff's overview of the US policies [17], PPD-21 on Critical Infrastructure Security and Resilience made no major changes in policy, roles and responsibilities, or programs. PPD-21, however, did order an evaluation of the existing public-private partnership model, the identification of baseline data and system requirements for efficient information exchange, and the development of a situational awareness capability. PPD-21 also called for an update of the National Infrastructure Protection Plan (NIPP), and a new Research and Development Plan for Critical Infrastructure, to be updated every four years.

While not yet making any changes in policy, roles and responsibilities, and programs, the text of PPD-21 did reflect the *increased interest in* ***resilience*** *and* ***the all-hazard approach*** that has evolved in CI policy over the last few years. It also updated sector designations. However, highlighting the energy and communications sectors due to their importance to the operations of other infrastructures. The directive also required the updated NIPP [19] to include a focus on the reliance of other sectors on energy and communications infrastructure and ways to mitigate the associated risk. The latest policies have also focused efforts on expanding the cyber security policies and programs associated with CIP.

An example of research initiative is the US National Infrastructure Simulation and Analysis Center (NISAC), which is a modelling, simulation, and analysis program within the Department of Homeland Security (DHS) [20]. NISAC comprises an emergency support centre in the Washington, D.C. area, as well as Modelling, Simulation and Analysis units at the Sandia National Laboratories (SNL), Los Alamos National Laboratory (LANL), and the Pacific Northwest National Laboratory (PNNL). Congress mandated that NISAC serve as a "source of national expertise to address critical infrastructure protection" research and analysis. NISAC prepares and shares analyses of critical infrastructure, including their dependencies, vulnerabilities, consequences, and other complexities, under the direction of the Office of Cyber and Infrastructure Analysis (OCIA). To ensure consistency with CIP priorities, NISAC initiatives and tasking requests are coordinated through the NISAC program office. NISAC provides strategic, multidisciplinary analyses of dependencies and the consequences of infrastructure disruptions across all sixteen US CI sectors at national, regional, and local levels.

NISAC experts have developed and are employing tools to address the complexities of dependent national infrastructure, including process-based systems dynamics models, mathematical network optimisation models, physics-based models of existing infrastructure, and high-fidelity agent-based simulations of systems.

The NISAC is managed by the Department of Homeland Security (DHS) Office of Cyber and Infrastructure Analysis (OCIA) to advance understanding of emerging risk crossing the cyber-physical domain. NISAC's Fast Analysis and Simulation Team (FAST) provides practical information within severe time constraints in response to issues of immediate national importance using NISAC's long-term planning and analysis results, expertise, and a suite of models including impact models. Formerly known as Department's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), FAST allows to assist in emergency planning by assessing CI resilience before and during a major emergency, e.g. a Katrina or Sandy-like hurricane.

3.2 Initiatives in Europe

Reducing the vulnerabilities of CI and increasing their resilience is one of the major objectives of the EU. The European Programme for Critical Infrastructure Protection (EPCIP) sets the overall framework for activities aimed at improving the protection of CI in Europe—across all EU States and in all relevant sectors of economic activity [21]. The threats to which the programme aims to respond are not only confined to terrorism, but also include criminal activities, natural disasters, and other causes of CI disruptions. In short, it seeks to provide an **all-hazards cross-sectorial** approach. The EPCIP is supported by regular exchanges of information between EU Member States in the frame of the CIP Contact Points meetings.

EPCIP focuses on four main areas [21]:

- The creation of a procedure to identify and assess Europe's CI and learn how to better protect them.
- Measures to aid protection of CI including the establishment of expert groups at EU level and the creation of the Critical Infrastructure Warning Information Network (CIWIN)—an internet-based communication system for exchanging information, studies, and best practices in Europe [22].
- Funding for over 100 CIP projects between 2007 and 2013. These projects focused on a variety of issues including national and European information sharing and alerting systems, the development of ways to assess the dependencies between ICT and electricity transmission networks, and the creation of a 'good practices' manual for CIP policy makers [23].
- International cooperation with European Economic Area (EEA) and European Free Trade Area (EFTA) nations, as well as expert meetings between the EU, USA, and Canada.

A key pillar of this programme is the 2008 Directive on European Critical Infrastructures [6]. It establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection. The Directive has a sectorial scope, applying only to the energy and transport sectors. The 2008 Directive also requires owners/operators of designated ECI to prepare Operator Security Plans (advanced business continuity plans) and nominate Security Liaison Officers (linking the owner/operator with the national authority responsible for CIP). Classified non-binding guidelines were also produced.

Taking into account the developments since the adoption of the 2006 EPCIP Communication [21], an updated approach to the EU CIP policy became necessary. Moreover, Article 11 of the 2008 Directive on the identification and designation of European Critical Infrastructures refers to a specific review process of the Directive. Therefore, a comprehensive review has been conducted in close cooperation with the Member States and stakeholders during 2012. In 2013, the European Commission evaluated the progress made by EPCIP and suggested the programme enter a new more practical phase for the future. This phase involves launching a pilot project analysing four European Critical Infrastructures (ECI) with regards to possible threats. These were:

- The EU's electricity transmission grid
- The EU's gas transmission network
- EUROCONTROL—the EU's Air Traffic Management
- GALILEO—the European programme for global satellite navigation.

Based on the results of this review and considering other elements of the current programme, the Commission adopted a 2013 Staff Working Document on a new approach to the EPCIP [24]. It sets out a revised and more practical implementation of activities under the three main work streams—prevention, preparedness and response. The new approach aims at building common tools and a common approach in the EU to critical infrastructure protection and resilience, taking better account of dependencies.

Compared with the US, the EU approach, though referring to national rather than EU legislation, seems to be a step forward towards regulative efforts instead of mere voluntary compliance, although both the US and the EU make emphasis on the importance of public-private partnerships.

In terms of cyber resilience, the European Commission has adopted a series of measures to raise Europe's preparedness to ward off cyber incidents. The Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [25], also known as the NIS-directive, is the first piece of EU-wide legislation on cyber security. The Directive focuses on three priorities: (a) Member States preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority; (b) cooperation among all the Member States, by setting up a cooperation group, in order to support and

facilitate strategic cooperation and the exchange of information among Member States; (c) a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICT, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of **essential services** will have to take appropriate security measures and to notify serious incidents to the relevant national authority. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the NIS-Directive. The European Commission is also examining how to strengthen and streamline cyber security cooperation across different sectors of the economy, including in cyber security training and education.

While there are similarities, the European Commission has not formally converged essential service operators and CI operators alike in [26]. Consequently, the EU Member States can adopt legislative solutions that allow a substantial coincidence of the two sets, or consider them as different set (with eventually some overlap).

In terms of research, the European Commission has funded over 100 diverse projects under the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks programme (CIPS), during the 2007–2012 period. The programme was designed to protect citizens and CI from terrorist attacks and other security incidents by fostering prevention and preparedness, namely by improving the protection of CI and addressing crisis management. The key objective is to support CIP policy priorities by providing expert knowledge and a scientific basis for a better understanding of criticalities and dependencies at all levels. A list of the EU co-funded projects can be found online [27]. Such projects integrate the more than 300 R&D projects co-funded by the EU Commission under the Security umbrella in the FP7 (i.e. the EU research funding agenda in the period 2007–2013). The programme covers all the aspects related with innovative technology for security, with a strong focus on security of CI. Amongst other projects co-funded under this framework is the Network of Excellence "Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet)" project [28].

The interest for EU Commission about the security issues is witnessed by the inclusion of the topic security also in the H2020 programme (i.e. the Horizon 2020 programme is the EU research funding agenda for the period 2014–2020) and by the more than 150 R&D projects already granted. To be more effective, H2020 shifted the focus from technology driven perspective to a problem solving orientation with a strong requirements of active involving of security stakeholders, starting from CI operators, in order to develop solution able to concretely increase the resilience, the robustness and/or the preparedness of EU society.

Finally, a European Reference Network for Critical Infrastructure Protection (ERNCIP) has been created by the European Commission to "foster the emergence of innovative, qualified, efficient and competitive security solutions, through

networking of European experimental capabilities". It aims to link together existing European laboratories and facilities, in order to carry out critical infrastructure-related security experiments and test new technology, such as detection equipment.

3.3 The Australian Approach

This Australian Government recognises the importance of CI and focuses its policy on the essential services for everyday life provided by parts of CI. In its 2010 CI Resilience Strategy, we observe a shift towards resilience that enables an all hazards approach [29]. The Australian strategy takes into account the dependencies between critical infrastructures and sectors. It defines resilience in the context of CI, as:

> Coordinated planning across sectors and networks, responsive, flexible and timely recovery measures, and development of an organisational culture that has the ability to provide a minimum level of service during interruptions, emergencies and disasters, and return to full operations quickly.

Like in the USA and Europe, the Australian Government aims to build a public-private partnership approach between businesses and government and has established the Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience (CIR) as its primary mechanism. The goal is to establish a cross-sector approach and the identification of cross-sector dependencies.

This strategy identifies six strategic aspects:

- operate an effective business-government partnership with critical infrastructure owners and operators
- develop and promote an organisational resilience body of knowledge and a common understanding of organisational resilience
- assist owners and operators of CI to identify, analyse and manage cross-sectorial dependencies
- provide timely and high quality policy advice on issues relating to CI resilience
- implement the Australian Government's Cyber Security Strategy to maintain a secure, resilient and trusted electronic operating environment, including for CI owners and operators, and
- support the CI resilience programs delivered by Australian States and Territories, as agreed and as appropriate.

While some of these activities are a continuation of the previous CIP Program, a new strategic imperative, the one of organisational resilience, emerges.

The Critical Infrastructure Program for Modelling and Analysis (CIPMA) is part of the Australian Government's strategy to: (a) reduce exposure to risk, (b) recover from major disruptions and disasters, (c) learn from incidents. CIPMA uses a vast array of data and information to model and simulate the behaviour of CI systems and how they interrelate. Governments and CI owners and operators can use CIPMA's modelling and analysis toolset and approach to help prevent, prepare for,

respond to, or recover from, a natural or human-caused disruption to CI. It draws on all its partners to do so, including other owners and operators of CI, state and territory governments, and Australian Government agencies. CIPMA also supports the work of the Trusted Information Sharing Network (TISN) for CI resilience. The network is a forum for owners and operators of CI and governments to share information.

4 CI Resilience

As we observed in the previous section, the Australian strategy has followed a clear direction towards CI Resilience (CIR). The main argument is that due to the adverse and changing landscape of hazards and threats to CI, it is not possible to foresee, prevent, prepare for or mitigate all of these events, which in several cases can be unknown or emergent. Moreover:

> Protective security measures alone cannot mitigate supply chain disruption, nor ensure the rapid restoration of services. Owners and operators of critical infrastructure often have limited capacity to continue operations indefinitely if the essential goods and services they require are interrupted [29].

As highlighted in [30], both the USPPD-21 [18] and NIPP 2013 [19] recognise CIP "as an enabler of CIR" (Critical Infrastructure Resilience). While the US approach currently recognises resilience alongside protection, or perhaps even emphasises the former at the cost of the latter [19], it is noteworthy that this approach places its emphasis on public-private partnership in the spirit of voluntary measures from the private side. This approach is different than the European policies, which focus more on regulatory measures.

In [30] it is highlighted that the Staff Working Document [24] already includes several references to the concept of resilience and it indeed uses the phrase "CI protection and resilience" frequently. Usually these two concepts are presented together, but the document does not explicitly define either of the concepts nor make it clear how they differ from each other and how they are related. In one occasion, however, when discussing the four "relevant pan-European critical infrastructures" that are to be used as European pilot projects from 2013 onwards, it is mentioned that the respective work streams "seek to provide useful tools for improving protection and resilience, including through providing for strengthened risk mitigation, preparedness and response measures".

Currently, there are not many national, official definitions of the concept of CI Resilience, but as we observed, several national policy and strategy reports include it as a key component in their CIP programs, which depicts a shift of the CIP field towards Resilience.

Looking at the different definitions and approaches, one can notice commonalities and differences [15]. Alsubaie et al. [31] observes that properties such as 'ability to recover' and 'ability to adapt' were incorporated in several definitions. Most of the proposed definitions include 'the ability to withstand' or 'absorb' a

disturbance as a key attribute. Similarly, Bruneau et al. [32] assigns four properties to resilience for both physical and social systems: robustness, redundancy, resourcefulness, and rapidity.

In another review of resilience concepts used for CI, Francis and Bekera [33] observes the evolution in the resilience concept and also concludes that the definitions seem to converge "in the direction of a common definition, as these definitions share several common elements: absorptive capacity, recoverability, adaptive capacity, and retention of identity (structure and functions)". They argue that the objective of resilience is to retain predetermined dimensions of system performance and identity or structure in view of forecasted scenarios.

Three resilience capacities, i.e. absorptive, adaptive, and restorative capacities [33, 34] are at the centre of these approaches and are linked with the various stages of typical infrastructure response cycle to disruption (before, during and after the event). In Francis and Bekera [33] the following resilience capacities for infrastructures are defined:

- **Absorptive capacity** refers to the degree to which a system can absorb the impacts of system perturbations and minimise consequences with little effort. In practice, though, it is a management feature depending on configuration, controls, and operational procedures. System robustness and reliability are prototypical pre-disruption characteristics of a resilient system.
- While absorptive capacity is the ability of a system to absorb system perturbations, **adaptive capacity** is the ability of a system to adjust to undesirable situations by undergoing some changes. A system's adaptive capacity is enhanced by its ability to anticipate disruptive events, recognise unanticipated events, re-organise after occurrence of an adverse event, and general preparedness for adverse events.
- **Restorative capacity** of a resilient system is often characterised by rapidity of return to normal or improved operations and system reliability. This capacity should be assessed against a defined set of requirements derived from a desirable level of service or control.

In their approach, Alsubaie et al. [31] recognise that it is important to take into account the inherent interdependencies that exist among most of the modern CI. In this respect, proposed resilience concepts and measures need to incorporate CI dependencies, considering the cascade of a failure through multiple CIs, which offer different services to the community. This dependency of resilience between communities and infrastructure has been widely recognised in the scientific literature [35] and is also depicted in the Australian CIP Strategy [29].

As pointed out in [15], resilience encompass **several dimensions**; such as *technical*, *organisational*, *social*, and *economic* ones. In summary, the technological dimension refers primarily to the physical properties of infrastructure components, systems, networks or 'system-of-systems' and refer to the characteristics and behaviour of these in the case of a change or incident. This dimension is very prominent when referring to engineering resilience or to CIR and it is the aspect

most of the modelling, simulation and analysis tools and approaches focus on. Another aspect relevant to CIR is the organisational one, as it relates to the organisations and institutions that manage the physical components of the systems, i.e. CI operators or owners. It covers aspects such as culture, people, business continuity, risk, and disaster management at the organisational level. This more business-oriented aspect, which we have observed in the Australian national policy, serves as a way to gather all current business practices under one common goal: the operability of the infrastructure under adverse circumstances. The social dimension encompasses population and community characteristics that render social groups either more vulnerable or more adaptable to hazards and disasters. We observe that national resilience policies recently include, except of economic or even environmental aspects, social aspects in their definitions of resilience as CI are vital for maintaining key societal functions. These refer to the community and highlight how infrastructures contribute with essential services to it, e.g. as discussed in the aforementioned NIS Directive.

Overall, a resilience-based approach for CI is an approach that is gradually adopted by nations in order to face the challenges and costs of achieving maximum protection in an increasingly complex environment and to overcome limitations of the traditional scenario-based risk management approach, where the organisation may lack capabilities to face risk from unknown or unforeseen threats and vulnerabilities.

5 Conclusion

This chapter introduced the concept of Critical Infrastructure (CI) and their protection. It has illustrated which factors contribute to the complexity of modern infrastructures, as well as the needs that drive scientists to develop modelling, simulation and analysis (MS&A) tools for this area. This interest in CI and complex systems is strongly related to initiatives, by several governments that from the end of the 90s of the previous century recognised the relevance of the undisturbed functioning of CI for the wellbeing of their population. They also stimulated the research community and gave rise to several projects, a selection of which was presented in this chapter.

In the past years, international policies and their respective research programs have shifted towards a resilience-based approach. While the different nations continue to work in areas such as risk management, protection, dependency modelling and analysis, etc., resilience gains a more prominent role, as the ‘umbrella’ term to cover all the various aspects and the various stages of crisis management when a critical infrastructure faces a disruptive event.

In the following chapters, we will focus on modelling, simulation and analysis and explore how such methods and tools can contribute to a better understanding of CI complexity and can be used in order to improve the protection and resilience of infrastructures.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312450.

The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author (s).

References

1. White House (1998) The Clinton's Administration's Policy on critical infrastructure protection: presidential decision directive 63/PDD-63, White paper, 22 May 1998. Available online at http://fas.org/irp/offdocs/pdd/pdd-63.htm. Retrieved on 27 Oct 2016
2. Rossignol M (2001) Critical infrastructure and emergency preparedness, report PRB 01-7E, Canada, June 2001. Available online at http://publications.gc.ca/Collection-R/LoPBdP/EB/prb017-e.htm. Retrieved on 27 Oct 2016
3. Brunner EM, Suter M (2008) International CIIP handbook 2008/2009. Center for Security Studies, ETH Zurich. Available online at http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf. Retrieved on 27 Oct 2016
4. CIPedia©, 2016. Available online at www.cipedia.eu. Retrieved on 27 Oct 2016
5. European Commission (2005) COM 576 final, Green paper on a European Programme for critical infrastructure protection, Brussels, 17.11.2005. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN. Retrieved on 27 Oct 2016
6. European Council (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), Brussels, Dec 2008. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN. Retrieved on 27 Oct 2016
7. Bologna S, Setola R (2005) The need to improve local self-awareness in CIP/CIIP. First IEEE international workshop on critical infrastructure protection (IWCIP'05). IEEE
8. Luiijf HAM, Nieuwenhuijs AH, Klaver MHA, van Eeten MJG, Cruz E (2010) Empirical findings on European critical infrastructure dependencies. Int J Syst Syst Eng 2(1):3–18
9. Van Eeten M, Nieuwenhuijs A, Luiijf E, Klaver M, Cruz E (2011) The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. Public Adm 89(2):381–400
10. US General Accounting Office (2003) Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants, report GAO-03-251, Washington DC, Feb 2003. Available online at http://www.gao.gov/new.items/d03251.pdf. Retrieved on 27 Oct 2016
11. OCIPEP (2002) The September 11, 2001 Terrorist attacks—critical infrastructure protection lessons learned, IA02-001, 27 Sept 2002, Ottawa. Available online at http://www.au.af.mil/au/awc/awcgate/9-11/ia02-001_canada.pdf. Retrieved on 27 Oct 2016
12. Nieuwenhuijs AH, Luiijf HAM, Klaver MHA (2008) Modeling critical infrastructure dependencies. In: Mauricio P, Shenoi S (eds) IFIP international federation for information processing. Critical infrastructure protection II, vol 290. Springer, Boston, pp 205–214
13. Setola, R, Luiijf E, Bologna S (2008) R&D activities in Europe on critical information infrastructure protection (CIIP). Int J Syst Syst Eng Nos. 1/2:257–270
14. Ouyang M (2014) Review on modeling and simulation of interdependent critical infrastructure systems. Reliab Eng Syst Saf 121:43–60

15. Theocharidou M, Melkunaite L, Eriksson K, Winberg D, Honfi D, Lange D, Guay F (2015) IMPROVER deliverable D1.2 first draft of a lexicon of definitions related to Critical Infrastructure Resilience, 30 Nov 2015
16. UNISDR Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction (UNISDR), Geneva, Switzerland, May 2009. Available online at http://www.unisdr.org/we/inform/publications/7817. Retrieved on 27 Oct 2016
17. Moteff JD (2015) Critical infrastructures: background, policy, and implementation, congressional research service, 7-5700, RL30153, 2015. Available online at https://www.fas.org/sgp/crs/homesec/RL30153.pdf. Retrieved on 27 Oct 2016
18. White House (2013) Presidential policy directive/PPD-21, critical infrastructure security and resilience, 12 Feb 2013. Available online at https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf. Retrieved on 27 Oct 2016
19. Department of Homeland Security, NIPP 2013: partnering for critical infrastructure security and resilience, 2013. Available online at https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf. Retrieved on 27 Oct 2016
20. Web page. Available online at http://www.sandia.gov/nisac/. Retrieved on 27 Oct 2016
21. European Commission, Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, COM (2006) 786 final—Official Journal C 126 of 7.6.2007. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN. Retrieved on 27 Oct 2016
22. Web page. Available online at http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm. Retrieved on 27 Oct 2016
23. Klaver M, Luiijf E, Nieuwenhuijs A (2016) Good practices manual for CIP policies for policy makers in Europe, TNO, 2011. Available online at http://www.tno.nl/recipereport. Retrieved 27 Oct 2016
24. European Commission, Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, Brussels, 28.8.2013, SWD (2013) 318 final. Available online at http://ec.europa.eu/transparency/regdoc/rep/10102/2013/EN/10102-2013-318-EN-F1-1.PDF. Retrieved on 27 Oct 2016
25. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ["NIS Directive"], Brussels, July 2016. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN. Retrieved on 27 Oct 2016
26. Luiijf E, van Schie T, van Ruijven T, Huistra, A (2016) The GFCE-MERIDIAN good practice guide on critical information infrastructure protection for governmental policy-makers. TNO. Available online at https://www.tno.nl/gpciip. Retrieved on 27 Oct 2016
27. European Commission, Examples of CIPS projects. Available online at http://ec.europa.eu/dgs/home-affairs/financing/fundings/projects/per-program/cips/index_en.htm#/c_. Retrieved on 27 Oct 2016
28. Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) website, 2016. Available online at www.ciprnet.eu. Retrieved on 27 Oct 2016
29. Australian Government (2010) Critical infrastructure resilience strategy. ISBN: 978-1-921725-25-8. Available online at: http://www.emergency.qld.gov.au/publications/pdf/Critical_Infrastructure_Resilience_Strategy.pdf. Retrieved on 27 Oct 2016
30. Pursiainen C, Gattinesi P (2014) Towards testing critical infrastructure resilience, EUR—Scientific and Technical Research reports, European Commission, Joint Research Center
31. Alsubaie A, Alutaibi K, Marti J (2016) Resilience assessment of interdependent critical infrastructure. In: Rome E, Theocharidou M, Wolthusen S (eds) Critical information infrastructures security, 10th international conference, CRITIS 2015, Berlin, Germany, 5–7 Oct 2015, Revised Selected Papers, pp 43–55

32. Bruneau M, Chang SE, Eguchi RT, Lee GC, O'Rourke TD, Reinhorn AM, Shinozuka M, Tierney AM, Wallace AM, Von Winterfeldt D (2003) A framework to quantitatively assess and enhance the seismic resilience of communities. Earthq Spectra 19(4):733–752. Available online at http://doi.org/10.1193/1.1623497. Retrieved on 27 Oct 2016
33. Francis R, Bekera B (2014) A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliab Eng Syst Saf 121:90–103. Available online at http://dx.doi.org/10.1016/j.ress.2013.07.004.367. Retrieved on 27 Oct 2016
34. Ouyang M, Dueñas–Osorio L, Min X (2012) A three–stage resilience analysis framework for urban infrastructure systems. Struct Saf 36–37, 23–31 May–July. Available online at http://dx.doi.org/10.1016/j.strusafe.2011.12.004. Retrieved on 27 Oct 2016
35. Melkunaite L (ed) (2016) IMPROVER deliverable D1.1 international survey, 31 May 2016. Available online at http://media.improverproject.eu/2016/06/IMPROVER-D1.1-International-Survey_DRAFT.pdf. Retrieved on 27 Oct 2016