Chapter

Analyzing the Cyber Risk in Critical Infrastructures

Marieke Klaver and Eric Luiijf

Abstract

Information and communication technology (ICT) plays an important role in critical infrastructures (CIs). Some ICT-based services are in itself critical for the functioning of society while other ICT elements are essential for the functioning of critical processes within CIs. Moreover, many critical processes within CIs are monitored and controlled by industrial control systems (ICS) also referred to as operational technology (OT). In line with the CI-concept, the concept of critical information infrastructure (CII) is introduced comprising both ICT and OT. It is shown that CIIs extend beyond the classical set of CIs. The risk to society due to inadvertent and deliberate CI/CII disruptions has increased due to the interrelation, complexity, and dependencies of CIs and CIIs. The cyber risk due to threats to and vulnerabilities of ICT and OT is outlined. Methods to analyze the cyber risk to CI and CII are discussed at both the organization, national, and the service chain levels. Cyber threats, threat actors, and the organizational, personnel, and technological cyber security challenges are outlined. An outlook is given to near future cyber security risk challenges, and therefore upcoming risk, stemming from (industrial) internet of things and other new cyber-embedded technologies.

Keywords: critical information infrastructure, cyber, risk, critical infrastructure, operational technology, industrial control systems, SCADA, internet of things, industrial internet of things, security, mitigation

1. Introduction

This chapter 'Analyzing the Cyber Risk in Critical Infrastructures' discusses the concepts of critical infrastructure (CI) and critical information infrastructure (CII), highlights the need for addressing the cyber risk to CI/CII, discusses methods and challenges in assessing the cybersecurity risk for CI/CII, and highlights upcoming cyber risk. This chapter brings together views on what comprises CII in the light of technological and societal developments, and how to analyze the cyber risk of CI and CII given the complexity of CI sector structures, dependencies, and service chains.

Following this introduction section, Section 2 introduces the concept of CII, its relation to the classical CI, and discusses the importance of analyzing the cyber risk to CI/CII. Section 3 discusses methods and challenges in analyzing the cyber risk to CI/CII both from the perspective of a single organization and across organizations e.g. across a CI sector or along a CI/CII service chain. Section 4 analyses the vulnerabilities and cyber risk of operational technology (OT) in CI. Section 5 discusses methods to analyze the cyber security risk across multiple organizations including

supply chains. Section 6 provides an outlook at new technological and regulatory developments and their possible impact on the cybersecurity risk for CI and CII. This chapter concludes with the conclusions in Section 7.

2. CI, CII, and the cyber risk

2.1 What is CI and how does that relate to CII?

The Council of the European Union has defined a CI 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*" [1]. Currently, many states on the globe have defined a subset of their infrastructure services as CI using similar definitions for CI. Their aim is to guarantee the wellbeing of their population and economy by safeguarding the undisturbed functioning of the society under all hazards. A list of national definitions for CI can be found at [2].

To determine their set of national CI sectors, states use methodologies such as a national risk assessment (NRA) method [3, 4] or a risk-based approach in combination with a set of criteria [5]. CI are deemed critical at the national level if e.g. the number of casualties or the economic loss caused by disruptions exceed certain thresholds [6]. Most states recognize energy, telecommunications and internet, drinking water, food and health as CI sectors [7]. Within these CI sectors, states identified critical processes, products, and services at the *national level.* Depending on its economic structure, historic developments, cultural, and other factors, states may recognize other sectors as CI, e.g. social services, monuments and icons as shown by the webpage 'critical infrastructure sector' on [2].

In line with CI, CIIs comprise those ICT-based elements for which the disruption or destruction may – according to defined criticality criteria - have a serious impact on a state's society and its economy. CII is therefore defined by [8] as "*those interconnected information and communication infrastructures, the disruption or destruction of which would have serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy*". Nevertheless, many states, which have defined their CI sectors, struggle in defining and accepting the concept of CII although the cyber risk to society extends beyond the classical set of CI sectors. Section 2.2 outlines the identification of CII and highlights why CIIs may extend beyond the currently identified national 'classical' sets of CI sectors.

2.2 Identifying CIIs

Alike the protection and resilience of CI, the protection and resilience of CII also starts with identifying CII. Many critical and essential services of our societies largely depend on the undisturbed functioning of underlying ICT and OT. According to [9], OT is "*the technology commonly found in cyber-physical systems that is used to manage physical processes and actuation through the direct sensing, monitoring and or control of physical devices*". The overarching term OT replaces many earlier notions for process control technologies to monitor and control cyber-physical processes (CPS): industrial control systems (ICS), distributed control systems (DCS), energy management systems (EMS), supervisory control and data acquisition (SCADA) systems, industrial automation and control systems (IACS), and process automation (PA) [10]. To mention a few applications of OT: the generation, transport and distribution of various modes of energy, refinery processes, building

DOI: http://dx.doi.org/10.5772/intechopen.94917

automation systems (air-conditioning, elevators, fire alarm system), physical security access (locks, gates, cameras), laboratory analysis systems, tunnel safety systems, harbor cranes, and automatic guided vehicles (AGV).

Identifying the ICT- and OT-based services that are critical for a state proves to be complex. Most states struggle in clearly understanding and defining the information infrastructure components of critical processes to the state and its population. CII elements and services are notoriously more difficult and complex to demarcate and define than CI, both technically, organizationally, and from a governance point of view.

CII elements tend to be more interwoven and tend to hide within a CI, in cyber-physical processes, and in stacks of information-based services. The speed of innovation and uptake of new digital technologies in processes that evolve into critical processes to the society is high. Obviously this is complex as the critical ICT- and OT-based functions and services hide themselves (1) in the IT-sector (telecommunication and internet), (2) classical sector-specific CIs (**Figure 1**), and (3) even beyond these established domains.

According to [11], CII comprise:

1. Critical elements and services of the ICT sector, for example mobile telecommunication data services, internet exchange points, domain name services, certificate infrastructures, and Global Navigation Satellite Systems such as Galileo, BeiDou, and GPS for Position, Navigation and Timing (PNT) services.

2. Critical information, communication, and operational infrastructure elements- ICT and OT- in each of the CI. This may include e.g. critical financial transaction systems in the financial sector, critical logistic information systems, and OT which monitor and control critical cyber-physical systems such as in gas transport, harbors, railways, healthcare, and refineries.

3. The products and services of manufacturers, vendors and system integrators which are used across multiple CI sectors, nationally and internationally, whose vulnerability or common cause failure may negatively impact the proper functioning of CII and the CI that they are a critical element of.

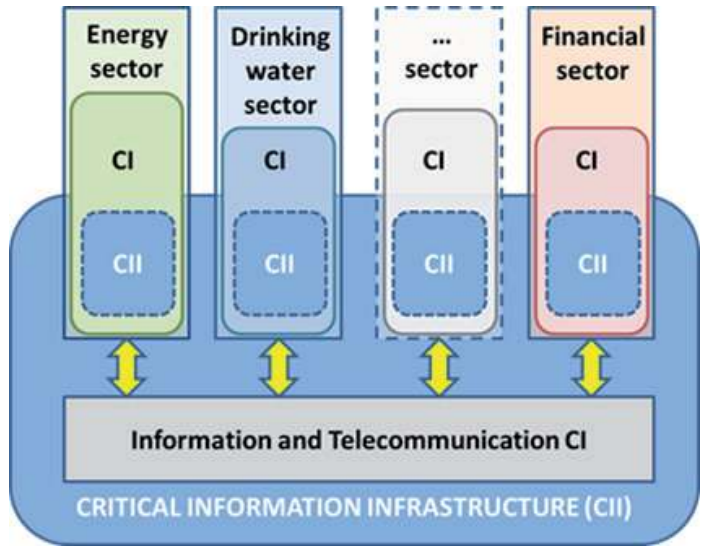

Figure 1.
Critical information infrastructure (source: [11]).

4. Critical ICT- and OT-elements and services beyond the established CI domains mentioned under (1) to (3) above. Such elements are often operated by organizations outside the classical ministerial supervision and/or regulation, may be physically located outside a state and or operated by foreign operators.

The extent of the nationally identified CII largely depends on the maturity and critical use of digital technologies by and in states (**Figure 2**). As a basis, essential CII elements include the ICT-based elements of the classical CI services such as electricity generation or drinking water. Digitally more advanced states have defined CIIs which have major elements outside the classical set of CIs. Due to the international nature of CII, the governance of CII protection and resilience extends beyond national borders and relies on international collaboration. Due to the increased role of ICT and OT in almost all other CI (e.g. cloud services, smart cities, smart grids), defining the CII requires cyclic updates to capture the dynamics inherently linked to ICT- and OT-based systems and networks. This process is complex due to the dynamics of the dependencies, and also to the sometimes-hidden nature of these dependencies, think e.g. on the dependency of electricity networks on the availability of precise timing and communication networks [12].

The EU, for instance, recognizes the need to secure both CI and CII in its European directive on security of network and information systems (NIS) [13]. The directive requires a higher level of cyber security by the operators of specific CI services in the energy (electricity, oil, and gas), transport (air, rail, over water, and road), banking, financial markets, health, drinking water supply and distribution, and digital infrastructure sectors. The non-classical CI 'digital infrastructure' comprises internet exchange points (IXs), domain name service providers (DNS), and top-level domain (TLD) name registries. EU Member States require by law that other national CI operators adhere to the same security requirements as well. Moreover, the NIS directive recognizes another set of CII operators: the digital service providers (DSPs). DSPs operate online marketplaces, online search engines, and cloud computing services when their operations exceed a certain size.

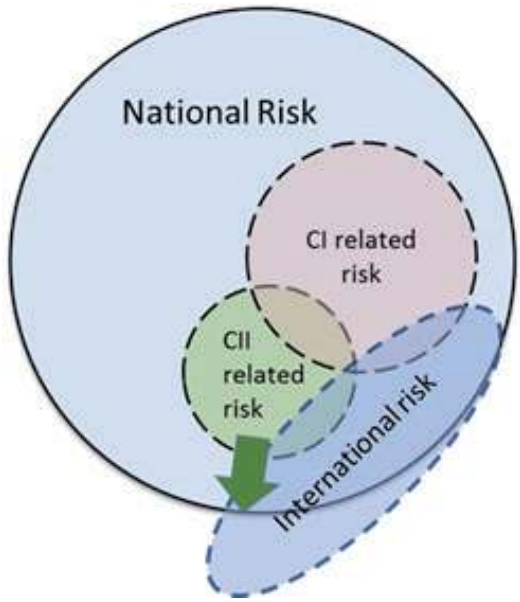

Figure 2.
Critical information infrastructure protection (CIIP): All activities aimed at ensuring the functionality, continuity, and integrity of CII to deter, mitigate and neutralize a threat, risk or vulnerability or minimize the impact of an incident. (source: [11]).

Moreover, the EU implicitly recognizes electronic identification and trust services for electronic transactions as CII in [14]. However, it should be noted that most EU states do not recognize their key registers on population, land, addresses and buildings, commercial companies, topology, and vehicles as CII [7].

The USA recognizes as life critical embedded systems as CII beyond the classical CI sectors: medical devices, internet-connected cars, and OT [15]. Other states, alike Australia, are in the process of identifying their CII.

The high dynamics of technological developments and subsequent societal use of ICT- and OT-based services, makes the identification of CII complex. What seems to be a new toy may become embedded in critical societal processes shortly. On the other hand, earlier critical services such as text messaging phase out while being replaced by newer mechanisms such as Whatsapp. Risk analysis and mitigation may be complex given (1) the ICT- and OT-technological dynamics, (2) the continuous shifts in the threat spectrum, and (3) new CII services often operated by new, non-traditional operators (e.g. cloud services) which do not fit automatically in the governance structures of states.

2.3 Why considering the cyber related risk to CI and CII?

The most feared phenomenon by states is the cascading effect due to dependencies between CIs and CIIs. When one CI or CII is disrupted or destroyed, cascading disruption(s) may occur through the dependency of other (critical) infrastructure(s). Another important risk factor to CI and CII is a common cause failure: "*a failure where the function of multiple infrastructures is disrupted or destroyed by the same cause or hazard affecting these infrastructures at the same location or area in the same time frame*" [2]. Common cause failures may for instance be triggered by extreme weather, flooding, wildfires, and common use of the same vulnerable ICT or OT application, software, or equipment.

In modern societies, the (cyber) risk to society and the economy due to inadvertent and deliberate CI/CII disruptions and cascading and common cause phenomena increases due to:

- The diminishing governmental control over classical CIs and CIIs due to liberalization and privatization of their operations.

- A more economic-based risk approach by CI and CII operators aiming for improved efficiency, productivity, and organization performance, as compared to a more societal risk-based approach by the earlier public CI/CII operators.

- The fast appearance of new ICT-based services that are perceived essential or even critical by society even before government considers them as being CII.

- The perceived critical use by citizens of new stacked services which make the underlying ICT-infrastructure critical, e.g. the mobile e-payment infrastructure.

- Urbanization which stresses the, often aging, CIs to the limits of their design capability and capacity.

- The increased dependence of CI on ICT and the hidden nature on some dependencies, see for instance [12] for possible cascading effects of disruptions of time synchronization services in electrical power networks.

- The increased use of vulnerable ICT and OT for the monitoring and control of CI operations.

- Complex dependencies of CI/CII services and the risk of cascading failures.

- The increased dependence of industries and the population on undisturbed CI and CII services. They expect and require a high level of CI/CII resilience, basically an undisturbed service 24 hours per day, all year around. Modern societies and its population cannot cope anymore with CI/CII service disruptions that affect a large area and have a long duration, citizens and businesses have no plan 'B'.

- The increased level of cyber-attacks by state actors [16] and other types of actors [17] deliberately performing (cyber) attacks on CIs and CIIs in support of their political and financial objectives. See e.g. the warning in [18].

- Vulnerabilities in commonly used ICT- or OT-applications and systems being the source of a common cause failure, e.g. a common vulnerability in a popular application may lead to vulnerabilities in many organizations simultaneously, see e.g. the Dutch national cyber security centre (NCSC) warning for a Citrix vulnerability [19].

- The high dynamics in vulnerabilities of ICT- and OT-applications and -systems.

Therefore, the analysis and mitigation of the cyber risk in CIs and CIIs pose major challenges to states and their operators of essential services.

3. Assess the cyber security risk in CI

3.1 CI, CII and risk analysis

Risk analysis is defined by the EU as the "*consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure*". [1] The Council of Europe's European Centre of Technological Safety (TESEC) defines risk analysis as: "*the determination of the likelihood of an event (probability) and the consequences of its occurrence (impact) for the purpose of comparing possible risks and making risk management decisions*" [20]. Identifying the cyber threat scenarios and vulnerabilities related to CIs and CIIs is an important element of the sectoral, national, and wider CI and CII protection and resilience policies and frameworks [13, 5–7]. Managing the characteristics requires thorough and regular assessments of the cyber risk for CIs and CIIs, both at the level of a single CI/CII operator, across a CI/CII sector, across CI/CII chains of services, and at the national level.

Risk assessment (RA) is "*the combination of vulnerability analysis and risk analysis*" leading to the "*determination and presentation (usually in quantitative form) of the potential hazards, and the likelihood and the extent of harm that may result from these hazards*" [20].

Risk analysis, vulnerability analysis, and, subsequently, RA are therefore important elements of the CI/CII protection and resilience efforts. Moreover, the risk management (RM) process for CI and CII should not only cover the business

perspective of the risk but should also cover the societal impact of the risk: what risk does society faces when a large-scale disruption occurs? This requires RAs at multiple levels of aggregation, each with a different objective:

- An operator of essential services (CI or CII) will primarily use RA to obtain an overview of possible risk factors that can harm its business objectives and profits. Legal requirements will be a mere boundary condition to this process. The cyber risk is just one aspect which is balanced with other risk aspects such as e.g. technical failure, lack of key personnel due to a pandemic, and adverse regulation.

- A RA at the CI/CII sector level will primarily focus on the resilience and reputation of the whole sector considering the individual mitigation measures taken by the operators within the sector. E.g. what is the risk of diminished trust by the population in e-banking?

- A RA for a specific CI or CII service which depends on a chain of intermediate services supplied by multiple service operators. The operator of the (end) service will primarily focus on the resilience of the whole service chain and the disruption risk due to failing or disruption of one or more of the intermediate services. The analysis will consider the individual resilience measures taken by the individual operators and the residual risk for the service chain.

- A RA at the national or regional level will primarily focus on risk with societal impact and will take a wider range than just CI and CII. A national or regional RA will e.g. also consider the risk of a pandemic outbreak or a large-scale flooding and will balance the outcomes with the cyber risk to CIs and CIIs. To assess this risk, various states use a National Risk Assessment (NRA) method to establish a balanced national risk view including the cyber risk, see e.g. [3, 4, 21–23].

Due to the importance of CIs and CIIs for societies, CI and CII sectors increasingly must analyze and assess their (cyber) risk regularly and systematically based on sector-specific regulations either imposed by the national regulator, e.g. [24], or through sector initiatives, e.g. the Basel III regulatory framework for the bank sector. The implementation of the EU NIS directive as discussed above requires CI and some of the CII operators to regularly perform RAs as a basis for their cyber security measures. RM is also a key element in the NIST framework [25].

Moreover, these CI and CII operators should be prepared to perform a quick reassessment of the cyber risk, mitigations, and the residual cyber-related risk in case a new cyber vulnerability or cyber threat comes to the fore.

3.2 Assessment of cyber risk by a single CI operator

The basis for the protection of CI lies in a strong RA at the operator level. For RA at the company level, including CI and CII operators, many methods and standards exist. Most of these methods are in line with the ISO 31000 series of RM standards [26]. For the IT-environment, ISO/IEC 27005 [27] provides the RM and risk mitigation background as part of the ISO/IEC 27000 series that assist organizations to implement information security management based on a set of terms and definitions [28] and security controls [29, 30]. For the OT-environment, security control frameworks with similar security control sets

exist, e.g. [31, 32]. Although these security control frameworks are often sector specific, they can be mapped on common structures or frameworks, see e.g. ENISA and NIST [25, 33].

One of the important factors to cover in a RA of CI/CII is the risk of ICT/OT as a vulnerability that may cause disruptions of CI/CII. This may involve the risk of technical failure or human mistakes, but also the cyber risk of malicious attacks. Given the criticality for states, even hybrid conflicts affecting CIs and CIIs are envisioned, see e.g. [34, 35]. An early example is the Crimea conflict. On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting many customers in Ukraine. In addition, there have also been reports of malware found in Ukrainian companies in a variety of their CI sectors [36].

Section 4 below specifically focusses on the cyber risk factors related to OT.

3.3 Assessment of the cyber risk across organizations

A RA for a specific CI sector is feasible, as was shown by the EUropean Risk Assessment and COntingency planning Methodologies for interconnected energy networks (EURACOM) project [37]. This approach extended the EUropean Risk Assessment Methodology (EURAM) [38] with contingency planning. In particular, chapter 4 of the EURACOM report discusses the cyber threats to the energy CI sector. The methodology is based on a common and holistic approach (end-to-end energy supply chain) for RA, RM and contingency planning across the power, gas, and oil CI subsectors.

The seven steps of the EURAM RA methodology are shown in **Figure 3**. The methodology scales from the department level to the operator level, to the CI or CII sector, and national level. Moreover, the methodology may embed the results of other RA methodologies. Risk which cannot be dealt with at a certain level may be input to the next higher level of abstraction. For example, the risk implications of a pandemic or a state actor cyber-attack to a nation cannot be managed alone by a CI operator and must be off-loaded to and managed at the national or even supranational level.

3.4 Challenges to assess ICT/OT risk across organizations

Although methods and approaches exist to perform RA across organizations. (e.g. a CI/CII sector or a service chain) some practical challenges exist:

- *The risk attached to ICT and OT elements across CI/CII-chains.* Certain CI/CII services are composed of a set of (chained) ICT and OT elements provided and operated by multiple operators. The criticality of certain elements to a CI or CII may be unknown to its operator; therefore, its protection has less priority than required from the national CI protection (CIP) or NIS point of view. It is a challenge to identify such critical elements and to assess the risk attached across the chain. In support of this type of assessments, new methods have been proposed, e.g. the RA method suggested by the Dutch cyber security council which requires the collaboration of all organizations in a supply chain to collectively assess the risk and define the appropriate security controls [39].

- *Identifying the risk related to critical elements in various CI/CII*: Some ICT and OT products are widely used across many CI and CII sectors and other organizations. The cyber risk attached to a systemic failure or vulnerability of such

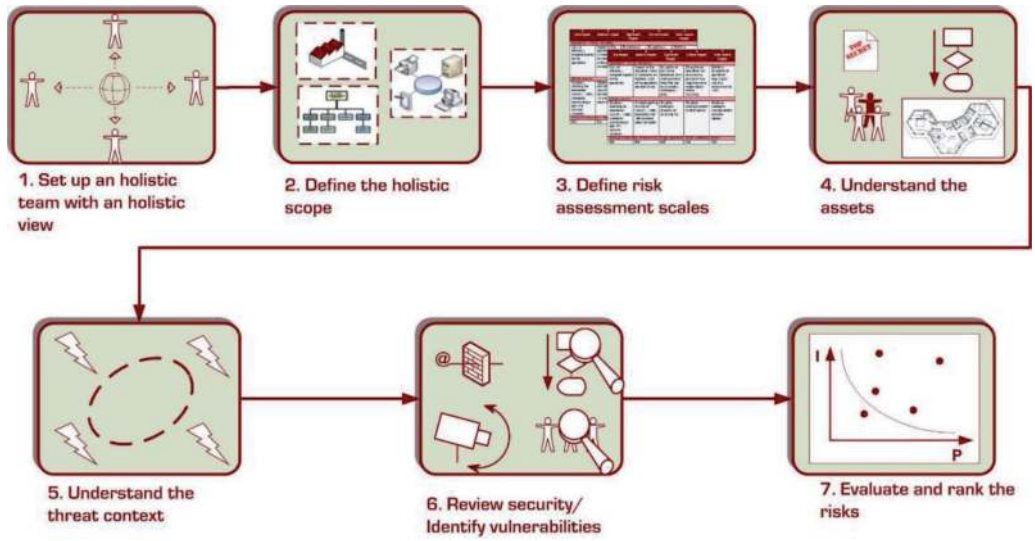

Figure 3.
The EUropean Risk Assessment Methodology (EURAM) approach (source: [38]).

a product may be large, e.g. a vulnerability in Microsoft Windows systems or in commonly used OT systems. Such a vulnerability may lead to a high level of risk at the national or even the international level. This risk is difficult to assess since it requires a detailed and well-maintained asset inventory of systems and applications used by each CI/CII operator.

- *The international nature of part of the CII:* Assessing the risk and taking mitigating measures for CIIP might be troublesome when the CII ownership, operations and or (operational) jurisdiction are beyond one's national border. Conflict of interests, legal requirements, and procedures may occur. For example, a cloud server operator having its operations in state B should report a cyber security breach to the national authority in that state. However, state A may have made regulation that each CII operator should report security breaches within 24 hours to them. When a CI operator in state A uses such a cloud service, the cloud service could have been designated as CII thereby imposing regulation on the cloud operator in state B. Such cross-border CII issues arise with the diverse national implementations of the EU NIS directive [40], and other CII-related laws. The new EU security strategy intends to address these issues [35].

These challenges lead to the necessity to perform RM not only at the company level but also across the service chain, and at the sector and national levels.

4. Assessing the OT risk

4.1 OT threats and vulnerabilities

To identify the main threats and vulnerabilities for the OT environment, a structured approach will be used in distinguishing multiple layers. Threats to OT may occur at multiple layers as defined by [41]:

- The governance layer.

- The socio-technical layer comprising the OT/ICT architecture, the technology, networking, and human factors.

- The operational-technical layer including (3rd party) maintenance.

According to [42], a threat to OT is the "*potential cause of an unwanted incident through the use of one of more OT, which may result in harm to individuals, a system, an organization, critical infrastructure and vital societal services, the environment or the society at large*".

The governance layer. At the governance layer, the first threat stems from the fact that OT is technically embedded in functionality. The management focusses on the functionality, e.g. provide drinking water. Therefore, many chief information security officers (CISOs) or equivalent executive level responsibilities largely neglect the cyber risk to OT which at the same time is a major risk to the functioning of the whole CI.

Moreover, there is major cultural difference between the IT department and other departments which use OT as part of the 24/7 functionality of their CI services. In addition, the IT department often has the cyber security mandate for the whole organization. "IT" develops the organization-wide cyber security policies (e.g. authentication and password policy, patch and anti-malware policies). Protection of the integrity, confidentiality, and privacy of information is a high priority. Therefore, "IT" may disrupt its operational services when required to install urgent patches. In their mindset, "IT" is key to the business of the whole organization; "*OT is just the department of grease, pumps, and valves, isn't it?*"

The OT department on the other hand optimizes the control of the physical processes and are less concerned with cyber security. Most often, "OT" has to use of the networks managed by "IT" for wide area connectivity and remote access. "IT" even may state the company-wide cyber security policy to comply with specific cyber security management standards such as the ISO/IEC 27000-series [28]. "OT" has to adhere to those policies while such cyber security standards and good practices have not been developed for a 24/7 operational environment. For example, blocking an account after three subsequent login errors is of no help when an operator needs to change production settings in the middle of the night during an operational crisis. Such dissimilar needs, policies, and service expectations between "IT" and "OT" can be a source of conflicts. Governance of OT security therefore requires efforts by all involved to bridge the gap between the ICT and OT domains.

Another governance level threat is that the economic depreciation of OT is often equal to that of the OT-controlled system, e.g. a water purification unit. Therefore, very aged control system components such as a 486 Windows/XP system still operate hidden in cabinets. They still control metros, sewage systems, and so on.

In other situations, the renewal of OT will be a long-term process where the upgrade will be performed (sub)process by (sub)process. This means that the central system control must cooperate with both new and legacy OT. Mixed configurations mean that cyber security measures cannot be activated at all or can only be effective on and between the new OT-systems and applications.

"*No worry about cyber security of OT, the processes still can be controlled manually*". At least management holds that view neglecting that the same management considerably reduced the experienced workforce able to manually operate the CI system. Therefore, an OT-disruption for longer than a couple of hours inevitably brings down the OT-controlled CI/CII services to society.

The socio-technical layer. At the socio-technical layer, [42] identifies a number of threats to the undisturbed functioning of OT-controlled CI processes, and therefore to the continuity, integrity and safety of physical processes. For example:

- Lack of cyber-security awareness of operators and other people operating and maintaining OT-controlled processes. No specific cyber-security education and training is part of their curricula.

- In the process control environment, it is not unusual that employees have been employed for many years. The risk of sabotage activities by disgruntled and dismissed employees is large. Many cases can be found in the media, e.g. the Maroochy water breach, and a sabotaged leak detection system of the Pacific Oil platforms and pipelines near Huntington Beach, USA. A risk which is not new: insider OT sabotage occurred already in the 90's, see e.g. [43].

The operational-technical layer. At the operational-technical layer, [42] identifies OT-specific threats including:

- The SCADA (and similar) protocols were designed in the 60's with a no threat, benign, closed operating environment in mind. Such protocols are not robust against any serious cyberattack. Applying such protocols now on top of TCP/IP increases the risk even more. A malformed packet may crash or lead to a dementia paralytica of process logic controllers as was shown by [44].

- The use of old technology and legacy OT, for reasons mentioned above, requires the need for personnel still knowing all ins and outs of twenty year or older OT as well as current technology. The old OT has no security-by-design. Moreover, old OT has too limited CPU and memory resources to run a malware protection package or encryption; the addition may break the critical process monitoring and control cycle. Moreover, a new plug-compatible board to replace a defective one may introduce new vulnerable functionality that is attractive to cyber attackers.

- In standard "IT" communications, temporary blocking of transmissions is accepted. In the OT-environment, however, not timely received status information from a process or a delayed control command may cause irreversible effects in the physical environment.

- OT systems may directly or indirectly be connected via remote operations or maintenance with the internet. Shodan [45] and similar search engine tools show ample OT-equipment that are directly accessible via the internet.

- System maintenance of OT in CI requires a lot of efforts due to the sheer size of the number of components. Password management policies, e.g. replacing passwords regularly, conflicts with the 24/7 operational continuity. CI sectors have agreed to good practices for patching and anti-malware signature updates but struggle with applying them, e.g. to apply security critical patches within a week after publication; all other patches to be applied during the next scheduled maintenance slot [46, 47]. In practice, patches are applied some three-quarter years after they became available and anti-malware signature files are updated after weeks if not months. "*If the controlled process works, do not break it*" is used as an excuse. Therefore, the risk of unauthorized exploitation of OT in CI sectors is high.

- Third party maintenance engineers are often given unrestricted and unmonitored access to key processes 24/7. Incidents have shown that third party employees cannot always be trusted.

4.2 Assessing the assurance of equipment and applications

A complex element in identifying the cyber risk in CII operations is assessing the risk in the wide variety of hardware and software CI operators use. Most CI/CII operators use ICT and OT from a multitude of suppliers, partly being global players. The hardware and software may contain hidden vulnerabilities. A CI/CII operator should try to ensure a high level of security of their own hardware, software, and services, and of those that are procured from suppliers. Organizations should adopt a security lifecycle approach to enhance the safe and secure functioning of their ICT elements. The security lifecycle comprises the acquisition, installation, system integration, operations, maintenance, upgrading, and decommissioning phases. When CI/CII operators are dependent on ICT and OT suppliers, system integrators, and third-party maintenance companies, they should have contractual agreements and measures in place to ensure that the resilience is up to par with the security requirements of the CI/CII organization. Based on the efforts of each organization, the use of cyber security standards and frameworks may increase the level of resilience across the chain. Examples of this approach are the third-party security requirements included in cyber security standards and frameworks [25, 29, 30, 32].

Assessing the level of assurance of each ICT/OT element, proves to be a challenge for an individual organization. Therefore, many organizations require support from their government, e.g. in certification of certain equipment. Recently, the EU Cyber Security Act [48] provides a framework structure for certifications, which is being taken up by ENISA and several of the European states although a number of challenges is perceived [49, 50].

4.3 Assessing the risk for the OT environment

The above-mentioned characteristics of OT systems, makes it necessary to include the following steps as part of the RA process:

- Use a multi-disciplinary team to assess the holistic risk to cyber. The team shall include those involved with general IT security, OT security, physical security, electronic security, security of services and supplies by utilities and third parties (e.g. power, external telecommunications, cooling), human resources (e.g. personnel security and safety).

- Collaborate with government organizations and relevant computer incident response teams (CSIRTs) on threat information and on assessing the risk to OT-equipment, software, and (tele)communication means.

- Identify the ICT and OT systems and networks that are critical to the key operational processes of the CI operator.

- Assess the impact of a disruption of ICT and OT to the CI service(s).

- Identify the connections with outside networks.

- Identify the external dependencies including third parties.

- Identify legacy systems that may pose additional vulnerabilities.

5. Assessing cyber security risk across CI/CII chains

Section 3.4 discussed the challenges for risk analysis across organizations in CI/CII chains. There exist several methods that support risk analysis across a chain of organizations which provide critical or essential services. There are, however, many challenges in applying such methods as is shown in Section 5.2.

5.1 Methods to assess the cyber risk across chains

Due to the specific characteristics, there is a need to perform RM not only at the company level but also perform a collaborative assessment across CI/CII service chains. There have been some studies that aim to establish a method for assessing the cyber-security risk across chains of CI/CII operations [38, 39].

The Dutch chain analysis method [39] has been developed by a set of CI operators in the energy sector. It was their believe that organizations in a supply chain together are in the best position to define and deploy appropriate controls and initiatives to reduce any cyber security risk themselves. The method aims to provide insight into the cyber security risk within a supply chain. It uses a layered approach to provide insight into the risk that arise from the ICT/OT systems and their interconnections as well as the potential risk that may pose to the chain of business processes of organizations. The identified risk in the business processes can ultimately disrupt the continuity of the entire supply chain of one or more critical or essential CI/CII services. By combining and merging the identified risk in business processes per organization, which should include their own third-party risk to these processes, the overall risk to the supply chain can be assessed (see **Figure 4**).

The aforementioned EURAM/EURACOM method uses a similar approach by combining three components to assess risk at an aggregated level, based on RAs by the individual organizations and is based on embedding lower level RA results by mapping the identified risk at the higher level [38].

Note that due to the hidden nature of ICT and OT within CI and CII, RM across the chain requires a large effort and a combination of expertise by all stakeholders

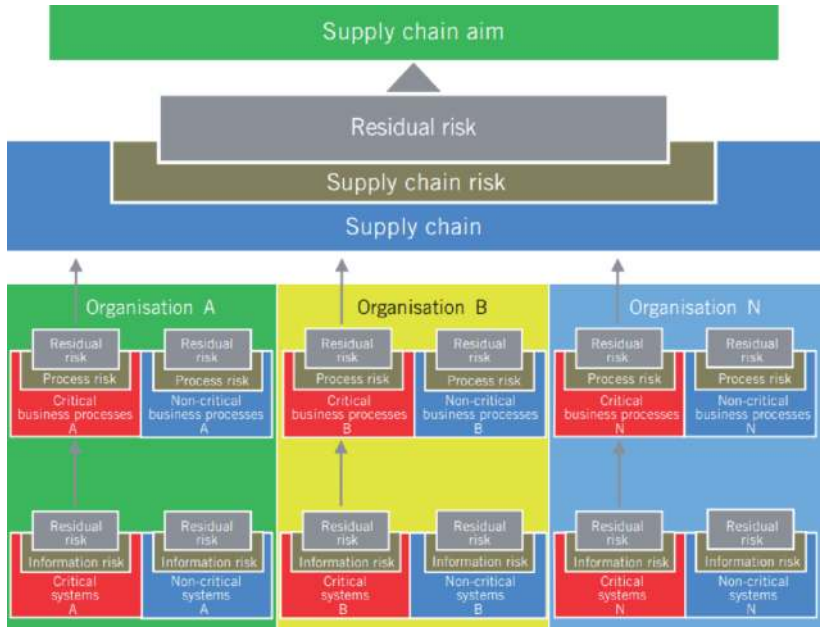

Figure 4.
Visualization of the Dutch supply chain risk management method (from [39]).

to assess this risk and define appropriate mitigating measures as is highlighted by the aforementioned Dutch supply chain RA pilot [39]: "*Providing insight into the cyber security risk within a supply chain requires a level of commitment of all organizations involved. It is paramount that in addition to the availability of adequate resources sufficient trust exists between organizations to share sensitive information among each other*."

5.2 Challenges to assess the cyber risk across CI/CII chains

In safeguarding CI and CII, cyber risk mitigation plays an important role. Cyber risk mitigation approaches comprise legal frameworks [13], the implementation of mostly non-CI/CII specific cyber security frameworks for ICT and OT [25, 29–32, 51], the sharing of cyber security information [52, 53], and a collaborative approach. The incentive for collaborative action to the cyber risk at the sector level and across service chains is clear. Resources are scarce and can be optimized by collaborating. Due to the interconnectedness of CI and CII, all organizations in a sector or service chain suffer when one weak link exists and fails, making a joint approach a necessity. Although many initiatives exist, the uptake of these initiatives is sometimes less than planned. Although there are methods available to assess the cyber risk across a CI chain, there exist challenges to apply those methods. Some of the factors that may prove a barrier in the adaptation of these methodologies are:

- *Different RA methodologies used by individual organizations:* Collaboration of RA across chains requires information sharing and discussions on the results of RA for the individual organizations. The sharing of information on the RA may be hampered when different methodologies are used. Although there are ways to overcome this, see e.g. [38], this requires some additional effort by the participating organizations.

- *Scarce resources:* Cyber security is a domain where expertise is still a scarce resource. When large scale incidents occur that would benefit from cross-organizational collaboration, many of the personnel needed will be taken-up by high-priority activities within their own organizations.

- *Difficulties in establishing effective public and private partnerships:* collaboration across the chain may require a close collaboration between public and private organizations, e.g. on information sharing on threats and vulnerabilities. While public-private partnerships (PPPs) are a popular form of collaboration in a number of states, in practice we see that they often lead to less than satisfactory results. Although the precise failure rate of PPPs in CIP is unknown, in the context of business-to-business partnerships failure rates of 30% up to 80% have been reported. This high failure rate may be based on tensions inherent to a PPP. Some balancing mechanisms are needed to overcome the inherent tensions [54].

- *Cross-border collaboration:* Most CI/CII operators use equipment of many different suppliers that originate worldwide. This may hamper information sharing and collaboration.

- *Legal barriers:* Anti-trust legislation on the one hand, and Freedom of Information (FOI) legislation on the other hand may create barriers to collaborate and exchange information between organizations [53].

- *Internal barriers:* Legal departments tend to block collaboration as they regard the shareholder risk too high due to negative image when information about cyber vulnerabilities or incidents leaks through partners [53].

6. What's next?

6.1 Trends and developments in CIIP

CIIP is an ongoing challenge for governmental policymakers and political leadership. Effective CIIP requires a constant assessment of future technological developments and keeping track of the dynamics in the ICT and OT domains. The increasing use of ICT and (embedded) OT to monitor and control critical and complex cyber-physical systems means that most CI have CII components or are slowly transforming into CII. Meanwhile, the cyber security of OT is lagging far behind that of ICT despite specific cyber security good practices and standards [32, 55]. However, the IEC 62443 framework on Security for industrial automation and control systems has recently been extended with a part on RA [31].

Developments in ICT and OT and their interrelationships continuously alter the nature of CI and CII, for instance big data, smart energy grids, autonomously driving vehicles, 5G, e-health monitoring, and remote robotic surgery. Keeping track of the dynamically changing cyber risk landscape for CI and CII is therefore a challenge. Chapter 6 of [56] states that the "*continuous developments in digital technology require states to keep track of the changing risk landscape and to review CIIP policy accordingly*". Moreover, Chapter 4 of [11] states that "*Horizon scanning strengthens CIIP policy as it enables nations to proactively signal and assess developments in technology, and to act when new technology reaches the potential to become part of the national CII.*"

Nevertheless, it is difficult to recognize developments in the criticality of information infrastructures due to the hyper-connectivity of modern technologies which suddenly may alter existing dependencies and introduce new dependencies within CIIs and between CII and CI. Dependencies may shift in unforeseen ways due to unanticipated adoption of traditional or seemingly unimportant information infrastructure elements. Such changes may cause other information infrastructure services to become critical to a state on the one hand and to cause the criticality of other CII elements to disappear over time on the other hand [57].

Similarly, company policy changes unexpectedly may affect CI/CII incident response and recovery plans for ICT and OT operations. Consider the organization's green policy to replace all vehicles by e-vehicles. The existing incident response and recovery plans which dispatches repair trucks and their crews over long distances during a long power disruption will fail when no special provisions for recharging during non-normal modes of operation are made and will delay the recovery of CIs/CIIs.

Mass adoption and integration of new technologies such as internet of things (IoT), industrial internet of things (IIoT), internet-of-medical-things (IOMT), robotics and artificial intelligence may, besides changing the nature of CI and CII, also increase the risk of cyber and hybrid attacks to CII [34, 35]. Ecosystems of not well-secured, hundreds of thousands, if not more, of internetted devices may fall victim of cyber criminals. Their combined power may be used to attack CI, CII and life-essential devices, e.g. by denial of service attacks and spreading malware [58]. CI/CII operators and states shall be aware of this risk in time and take precautionary actions. For instance, smart grid technologies are fundamentally changing the

energy sector and may introduce new CII elements at the national level. With the advancements in sensory, actuator and wireless technologies as well as the global internet, the usage of OT expands rapidly towards IIoT. The need for cyber security by design in new technological developments such as robotics and AI most often is an afterthought. This increases the cyber risk to CI, CII and humans, e.g. the use of robotic equipment such as vehicles and as human assistants in dangerous CI environments [59]. Moreover, new technologies enter the organization via the backdoor and is part of CI/CII services before the cyber risk is assessed and mitigated in a proper way.

6.2 Laws and regulations

The global cyber risk makes that states develop strategies, laws and regulations to get more grip on the cyber security risk to their state. Apart from the European general data protection regulation (GDPR) that became fully into effect in all EU Member States on May 25, 2018 [60], CI and some CII operators may be designated as operator of essential services (OES) or DSP as a result of the national law and related regulations which implement the EU NIS directive [13]. Whether one is designed as an OES or DSP depends on the service(s) provided, size of the operations, number of customers, area, and the level of criticality as laid down in national ruling. One requirement is that the OES or DSP shall notify the competent authority or the CSIRT with national authority without undue delay of any incident having a substantial impact on the provision of services. Moreover, national law may oblige notification by an OES to the 'CI stovepipe' responsible ministry or regulator. In case personal data is involved, the GDPR notification is required as well. Non-compliance with the law may result in a huge fine.

Reporting cyber incidents may lead to more transparency on the actual level of the cyber risk and may lead that to more awareness with operators and policymakers on the risk that cyber threats and vulnerabilities pose for society.

7. Conclusions

Analyzing the cyber risk in CI and CII, firstly requires the identification of CII using a set of (nationally) established criteria. RA for CI and CII may take place at multiple levels: by the organization of the CI/CII operator, by the CI/CII sector, nationally across all CI/CII sectors, and along the critical and essential service supply chains. This chapter provided insight to the OT risk, identifies the need for RA across organizations, and describes some RA models to address the cyber risk across multiple organizations and for service supply chains.

In assessing the cyber risk to CI/CII at the operator level, both ICT and OT should be considered. There exist many CI/CII sector-specific security control standards which can be mapped on common structures or frameworks as has been shown by e.g. NIST and ENISA. Although many standards and control measures exist, the OT risk at the governance, socio-technical, and operational-technical layers is often less understood and addressed by organizations. Recent advisories by government agencies show that the need to address the OT risk has become more urgent since the number of malicious attacks on OT as well as hybrid threats are growing while disruptions of the OT may have a large impact on the physical CI processes.

Recent research on RA for CI emphasizes on taking CI dependencies into account. This proves to be even more urgent and complex for CII. RA for CIIs and their dependencies is complex due to the highly dynamic nature of advances in and use of IT and OT, the often hidden nature of technological dependencies, think e.g.

about PNT services, and inclusion of embedded systems. Several RA approaches and methods exist to assess the cyber risk across organizations. However, assessing the cyber risk to the CI/CII service supply chains proves to be complex as it requires trust and willingness of all organizations involved.

And last not but least, organizations need to consider the cyber risk of future technologies before such technologies creep in via the backdoor and are an essential part of their critical services and business operations. The introduction of these new technologies can be planned (e.g. in the case of smart grids), which allows for an upfront analysis of the security risk involved, even when this risk is not always fully considered. New technologies, e.g. IoTs and dependencies may also be introduced in a more haphazard way into traditionally well-separated environments of CI/CII operators. Managing this additional risk is a major challenge for the operators.

Author details

Marieke Klaver[1*] and Eric Luiijf[2]

1 TNO Defence, Safety and Security, The Hague, The Netherlands

2 Luiijf Consultancy, Zoetermeer, The Netherlands

*Address all correspondence to: marieke.klaver@tno.nl

References

[1] The Council of the European Union. 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. Off J Eur Union [Internet]. 2008;L345:75-82. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[2] CIPedia(c) [Internet]. [cited 2020 Sep 16]. Available from: http://www.cipedia.eu

[3] Ministry of Security and Justice. Working with scenarios, risk assessment and capabilities [Internet]. The Hague, Netherlands; 2009. Available from: http://www.itineris.nl/?mdocs-file=4987

[4] Pruyt E, Wijnmalen D. National Risk Assessment in The Netherlands. In: Ehrgott M, Naujoks B, Stewart TJ, Wallenius J, editors. Multiple Criteria Decision Making for Sustainable Energy and Transportation Systems [Internet]. Berlin, Heidelberg: Springer Berlin Heidelberg; 2010. p. 133-43. Available from: https://www.researchgate.net/publication/226282956_National_Risk_Assessment_in_The_Netherlands/stats

[5] Theocharidou M, Giannopoulos G. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach [Internet]. Ispra, Italy; 2015. Available from: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf

[6] Theocharidou M, Kotzanikolaou P, Gritzalis D. Risk-Based Criticality Analysis. In: Palmer C, Shenoi S, editors. Critical Infrastructure Protection III. Berlin, Heidelberg: Springer Berlin Heidelberg; 2009. p. 35-49.

[7] Critical Infrastructure Sector [Internet]. [cited 2020 Jul 23]. Available from: https://websites.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure_Sector

[8] OECD. OECD Recommendation of the Council on the Protection of Critical Information Infrastructures Organisation for Economic Co-operation and Development C(2008)35. 2008.

[9] Boyes H, Isbell R. Code of Practice Cyber Security for Ships. London, United Kingdom; 2017.

[10] Colbert EJM, Kott A, editors. Cyber-security of SCADA and Other Industrial Control Systems [Internet]. Vol. 66. Boston, MA, USA: Springer; 2016. 354 p. Available from: http://link.springer.com/10.1007/978-3-319-32125-7

[11] Luiijf E, Van Schie T, Van Ruijven T. Companion Document to the GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. The Hague, The Netherlands; 2017.

[12] Stergiopoulos G. Power Sector Dependency On Time Service [Internet]. Heraklion, Greece; 2020. Available from: https://www.enisa.europa.eu/publications/power-sector-dependency/at_download/fullReport

[13] European Commission. 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 [Internet]. Brussels, Belgium; 2016. Available from: http://data.europa.eu/eli/dir/2016/1148/oj

[14] Council of the European Union. Regulation (EU) No 910/2014 of

the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [Internet]. Vol. 57, Official Journal of the European Union. Brussels, Belgium; 2014. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910

[15] Cybersecurity and Infrastructure Security Agency. Information Technology Sector [Internet]. 2020 [cited 2020 Oct 26]. Available from: https://www.cisa.gov/information-technology-sector

[16] DHS. Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar [Internet]. Washington, DC, USA; 2019. Available from: https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf

[17] De Bruijne M, Van Eeten M, Hernández Gañán C, Pieters W. Towards a new cyber threat actor typology: A hybrid method for the NCSC cyber security assessment [Internet]. The Hague, The Netherlands; 2017. Available from: https://www.wodc.nl/binaries/2740_Volledige_Tekst_tcm28-273243.pdf

[18] NSA, CISA. Cybersecurity Advisory NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems [Internet]. Washington, DC, USA: NSA and CISA; 2020. p. 1-5. Available from: https://media.defense.gov/2020/Jul/23/2002462846/-1/-1/1/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF

[19] NCSC. UPDATE: Vele Nederlandse Citrix-servers kwetsbaar voor aanvallen | Digital Trust Center [Internet]. The Hague, The Netherlands: National Cyber Security Centre; 2020. Available from: https://www.digitaltrustcenter.nl/nieuws/update-vele-nederlandse-citrix-servers-kwetsbaar-voor-aanvallen

[20] Budin G, Gréciano G, Rothkegel A, Hass U. Gestion du Risque pour usagers francophones [Internet]. Strasbourg, France; 2007. Available from: http://www.europhras.org/Site/anderedokumente/GMLGR5L_6_12_07.pdf

[21] Cabinet Office. Fact Sheet 2: National Security Risk Assessment [Internet]. London, United Kingdom; 2010. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62484/Factsheet2-National-Security-Risk-Assessment.pdf

[22] Trimintzios P, Gavrila R. National-level Risk Assessments [Internet]. Heraklion, Greece; 2013. Available from: https://www.enisa.europa.eu/publications/nlra-analysis-report/at_download/fullReport

[23] Public Safety Canada. All Hazards Risk Assessment Methodology Guidelines [Internet]. Ottawa, Canada; 2013. Available from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ll-hzrds-ssssmnt/ll-hzrds-ssssmnt-eng.pdf

[24] European Commission. Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010 (Text with EEA relevance.). OJ L 280, 28102017 [Internet]. 2017;1-56. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.280.01.0001.01.ENG&toc=OJ:L:2017:280:TOC

[25] NIST. Framework for Improving Critical Infrastructure Cybersecurity version 1.1 [Internet]. Gaithersburg, MD, USA; 2018. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[26] ISO. ISO 31000:2018 Preview Risk management -- Guidelines [Internet]. Geneva, Switzerland; 2018. Available from: https://www.iso.org/standard/65694.html

[27] ISO/IEC. ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management [Internet]. Geneva, Switzerland; 2018. Available from: https://www.iso.org/standard/75281.html

[28] ISO/IEC. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary [Internet]. Geneva, Switzerland; 2018. Available from: https://www.iso.org/standard/73906.html

[29] ISO/IEC. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements [Internet]. Geneva, Switzerland; 2013. Available from: https://www.iso.org/standard/54534.html

[30] ISO/IEC. ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls [Internet]. Geneva, Switzerland; 2013. Available from: https://www.iso.org/standard/54533.html

[31] IEC. IEC 62443-3-2:2020: Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design. Geneva, Switzerland; 2020.

[32] Stouffer K (NIST), Lightman S (NIST), Pillitteri V (NIST), Abrams M (MITRE), Hahn A (WSU). NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security [Internet]. Gaithersburg, MD, USA; 2015. Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[33] ENISA. Mapping of OES Security Requirements to Specific Sectors Mapping of OES Security Requirements to Specific Sectors About ENISA Mapping of OES Security Requirements to Specific Sectors [Internet]. Heraklion, Greece; 2017. Available from: www.enisa.europa.eu

[34] Niglia A, editor. Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges. Amsterdam, The Netherlands: IOS Press; 2020. 172 p.

[35] European Commission. Communication on the EU Security Strategy COM(2020) 605 final [Internet]. Vol. 53, Communication. Brussels, Belgium; 2019. Available from: https://ec.europa.eu/info/sites/info/files/communication-eu-security-union-strategy.pdf

[36] US-CERT. IR-ALERT-H-16-043-01AP CYBER-ATTACK AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE [Internet]. Washington, DC, USA; 2016. Available from: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[37] EURACOM. EURACOM Deliverable D2.3 - Integrated report on the link between Risk Assessment and Contingency Planning Methodologies [Internet]. Brussels, Belgium; 2010. Available from: https://docplayer.net/27429604-Deliverable-d2-3-integrated-report-on-the-link-between-risk-assessment-and-contingency-planning-methodologies.html

[38] Klaver MHA, Luiijf HAM, Nieuwenhuijs AH, Cavenne F, Ulisse A, Bridegeman G. European risk assessment methodology for critical infrastructures. In: Herder P, editor. 2008 First International Conference on Infrastructure Systems and

Services: Building Networks for a Brighter Future (INFRA) [Internet]. Rotterdam,The Netherlands: IEEE; 2008. p. 1-5. Available from: https://www.researchgate.net/publication/251883551_European_risk_assessment_methodology_for_critical_infrastructures

[39] Voster W, Mathijssen HH, Bloemen P, Beumer M, Dekker A, Mathijssen HH, et al. Cyber security supply chain risk analysis [Internet]. Dutch Cyber Security Council. The Hague, The Netherlands; 2015. Available from: https://www.cybersecurityraad.nl/binaries/Cybersecurity_supply_chain_risico-analyse_ENG_tcm107-323429.pdf

[40] ENISA. State-of-play of the implementation of the NIS Directive [Internet]. 2020 [cited 2020 Oct 30]. Available from: https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive

[41] Berg J van den, Zoggel J van, Snels M, Van Leeuwen M, Boeke S, Koppen L van de, et al. On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. In: NATO, editor. NATO STO/IST-122 symposium in Tallin, Estonia [Internet]. Paris, France: NATO RTA; 2014. p. 1-10. Available from: https://www.csacademy.nl/images/MP-IST-122-12-paper-published.pdf

[42] Luiijf E. Threats in Industrial Control Systems. In: Colbert EJM, Kott A, editors. Cyber-security of SCADA and Other Industrial Control Systems. Spinger; 2016. p. 69-94.

[43] RISI. Computer Sabotage at Nuclear Power Plant [Internet]. [cited 2018 Mar 3]. Available from: http://www.risidata.com/Database/Detail/computer_sabotage_at_nuclear_power_plant

[44] Lüders S. Control Systems under Attack? In: 10th ICALEPCS Int Conf on Accelerator & Large Expt Physics Control Systems Geneva, 10-14 Oct 2005, FR24-6O [Internet]. Geneva. Switzerland; 2005. p. 6. Available from: https://accelconf.web.cern.ch/accelconf/ica05/proceedings/pdf/O5_008.pdf

[45] Shodan [Internet]. [cited 2020 Sep 16]. Available from: https://www.shodan.io/

[46] UvW (Unie van Waterschappen). Baseline Informatiebeveiliging Waterschappen: Informatiebeveiliging Waterschappen Strategisch en Tactisch normenkader WS versie 1.0 [Internet]. Den Haag; 2013. Available from: https://www.uvw.nl/wp-content/uploads/2013/10/Baseline-Informatiebeveiliging-waterschappen-2013.pdf

[47] NERC. CIP-007-6 — Cyber Security – Systems Security Management Standard Development Timeline [Internet]. Washington DC, USA; 2014. (CIP). Available from: https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-007-6&title=Cyber Security - System Security Management

[48] European Commission. Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation [Internet]. Official Journal of the European Union Brussels, Belgium; 2019 p. 15-69. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[49] ENISA. Challenges of security certification in emerging ICT environments [Internet]. Heraklion, Greece; 2016. Available from: https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments

[50] ENISA. Considerations on ICT security certification in EU Survey Report [Internet]. Heraklion, Greece; 2017. Available from: https://www.enisa.europa.eu/publications/certification_survey

[51] JTF. Security and privacy controls for federal information systems and organizations Rev 5. Vol. 800, NIST Special Publication. Gaithersburg, MD, USA; 2020.

[52] ENISA. Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches [Internet]. Heraklion, Greece; 2015. Available from: https://www.enisa.europa.eu/publications/cybersecurity-information-sharing/at_download/fullReport

[53] Luiijf E, Kernkamp A. Sharing Cyber Security Information, Good Practice Stemming from the Dutch Public-Private-Participation Approach, The Hague, Netherlands. 2015.

[54] Klaver MHA, Vos P, Tjemkes B, Verner DR. Enhancement of Public-Private Partnerships within Critical Infrastructure Protection Programs. The Hague, Netherlands; 2017.

[55] DHS (Department of Homeland Security). Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies [Internet]. Washington, DC, USA; 2016. Available from: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[56] Luiijf, H., van Schie T, van Ruijven T, Huistra A. The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. The Hague, The Netherlands: TNO; 2016.

[57] Luiijf E, Klaver M. Governing critical ICT: Elements that require attention. Eur J Risk Regul. 2015;6(2):263-70.

[58] De Donno M, Dragoni N, Giaretta A, Spognardi A. DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation. Bugliesi M, editor. Secur Commun Networks [Internet]. 2018;2018:7178164. Available from: https://doi.org/10.1155/2018/7178164

[59] Steijn W, Luiijf E, Beek D van der. Emergent risk to workplace safety as a result of the use of robots in the work place [Internet]. Utrecht, The Netherlands; 2016. Available from: http://publications.tno.nl/publication/34622295/QDXZqU/steijn-2016-emergent.pdf

[60] European Commission. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da [Internet]. Brussels, Belgium; 2016. Available from: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679