Henrik P. Beckvard
DOI:10.33179/BSV.99.SVI.11.CMC.24.2.1

ZAŠČITA KRITIČNE IN KRITIČNE INFORMACIJSKE INFRASTRUKTURE

PROTECTING CRITICAL INFRASTRUCTURE AND CRITICAL INFORMATION INFRASTRUCTURE

Povzetek Ne glede na to, kako sta kritična infrastruktura in kritična informacijska infrastruktura kot njen del opredeljeni, sta obe nujni za delovanje, celovitost in varnost digitalizirane družbe. Opredeljevanje kritične informacijske infrastrukture in ocenjevanje tveganj ter nevarnosti, povezanih z njo, je prvi korak k zaščiti, skupaj z odločitvijo, da se tveganje zmanjša, odpravi ali sprejme. Za zaščito kritične informacijske infrastrukture je treba uskladiti prizadevanja in sodelovanje med resorji, ki so med seboj pogosto odvisni. Pri tem so pomembna javno-zasebna partnerstva in sodelovanje znotraj organizacij, kot sta Nato in EU.

Ključne besede ***Odpornost, kritična infrastruktura, sodelovanje med EU in Natom, javno-zasebna partnerstva, politika kibernetske varnosti.***

Abstract Regardless of how you define critical infrastructure, and critical information infrastructure as part of it, these are elements necessary for the functioning, integrity and security of a digitised society. Mapping what is critical (information) infrastructure and assessing the risks and hazards to it is a first step towards protection, along with a risk decision to either mitigate, remediate or accept the risk. For the protection of critical (information) infrastructure it is necessary to coordinate efforts and collaboration between sectors, which are often interdependent. Public-Private-Partnerships (PPP) and cooperation within organizations such as NATO and the EU are essential.

Key words ***Resilience, critical infrastructure, NATO-EU cooperation, public-private-partnerships, cyber security policy.***

Introduction

It is hardly possible to walk through the ruins of ancient civilisations without noticing the remains of infrastructure such as roads, ports, bridges, canals, aqueducts, dams and so on, all of which formed part of that society's infrastructure. Whenever infrastructure critical for the functioning of a society has been developed, steps to protect it have also been made (Assante, 2009). With the industrial revolution, and later the tech revolution, more layers have been added, but the protection of critical infrastructure is, in itself, nothing new. What sparks the current debate about strengthening the critical infrastructure sectors is, therefore, rather the amount of infrastructure that needs to be defended, the type of threats posed towards it, and the current geopolitical tensions that add to the urgency.

With the growing digitalisation and reliance on information technology (IT), and its linkage with operational technology (OT) devices controlling physical systems, »information« is today an ingrained part of critical infrastructure, and the term Critical Information Infrastructure Protection (CIIP) has become part of our vocabulary and thinking.

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) conducts a week-long course in Critical Information Infrastructure Protection (CIIP) together with the Defense Information Systems Agency (DISA)[1], intended for mid-level managers responsible for the protection of critical information infrastructure. The purpose of the course is to provide students with the knowledge necessary to analyse, assess and make decisions relative to CIIP. This article does not substitute the course, but may perhaps serve as an appetiser for delving more into the processes connected with the protection of critical infrastructure (CI) and critical information infrastructure (CII).

As will be discussed, the protection of CI and CII to a large degree depends on coordination and collaboration between agencies and other stakeholders – both civilian and military, private and public. No two countries or societies are quite the same, so how the protection is carried out may vary from country to country. The purpose of this article is therefore to describe the generic aspects of CI and CII protection, and to shed light on how this protection may be carried out.

1 WHAT CONSTITUTES CRITICAL INFRASTRUCTURE AND CRITICAL INFORMATION INFRASTRUCTURE?

Before discussing what is needed for its protection, it may be appropriate to define what constitutes critical infrastructure (CI) and critical information infrastructure (CII). Most nations have their own definitions and, not surprisingly, there is no universally recognised definition of CI or CII. In the United Kingdom, the term critical national infrastructure (CNI) is used to describe *those facilities, systems,*

[1] *The Defense Information Systems Agency (DISA) is a United States Department of Defense (DoD) combat support agency composed of military personnel, federal civilians, and contractors.*

sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example) (CPNI, 2021).

As not everything within a national infrastructure sector is judged to be 'critical', the UK government's official definition of CNI is:

»Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a) *Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or*

b) *Significant impact on national security, national defence, or the functioning of the state«* (CPNI, 2021).

Whether or not the critical infrastructure is »national« or simply has a national impact may be a matter of semantics. For instance, undersea cables may today be owned and operated by large companies such as Google, Facebook, Amazon or Microsoft, who have laid thousands of miles of cables along the seafloor, stretching between continents, to carry data around the world (INSIDER, 2021). In other words what is deemed to be critical infrastructure for a nation may not always be nationally owned, or even fully controlled.

Following the 9/11 attacks the United States of America, in its Patriot Act (2001), defined critical infrastructure as those *»systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.«*

According to EU Directive 2008/114/EC, »*'critical infrastructure' means 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«*.

Regardless of the definition, CI may be deemed as the elements essential for the functioning, integrity and security of a society. Equally, there are many definitions of critical information infrastructure (CII). The Estonian Information Systems Agency (RIA) defines CII as *»…information and communications systems whose*

maintenance, reliability and safety are essential for the proper functioning of a country. The critical information infrastructure is a part of the critical infrastructure.«

(RIA, 2021).

The European Union Agency for Cybersecurity (ENISA) has a slightly different definition stating that »*the definition of CII is taken from the Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection: ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc.)«* (ENISA, 2021).

In the Critical Information Infrastructure Protection (CIIP) course conducted at the CCDCOE together with DISA, we generally maintain that CII »*includes, but is not limited to:*

– *Terrestrial and undersea cable infrastructure*
– *Internet exchange points and commercial points of presence*
– *Satellite constellations*
– *Multiple disparate networks«* (Ruonavar, 2018)

Even though definitions vary slightly it may be concluded that with the level of digitalisation today CII is an integral part of CI, which is why areas such as power supply, internet exchange points and telecommunications will remain high on the list of CI.

Ultimately, what constitutes CI also varies from country to country depending not only on, for instance, the type of industry and power sources they have, but also on geography (e.g. a land-locked state may not have listed a sea port as CI). Most countries divide their CI into sectors.

As an example the UK has 13 Critical National Infrastructure (CNI) sectors listed: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water.

In contrast, the US has 16 Critical Infrastructure (CI) sectors: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems and Water and Wastewater Systems.

As there are a great number of mutual interdependencies between sectors, there is obviously also a need for coordination and collaboration between sectors – and

in some cases also between countries[2]. How to facilitate this coordination and collaboration, and who should take the lead in this process, will be dealt with in Section 4 below.

2 WHAT ARE THE RISKS TO CRITICAL INFRASTRUCTURE?

There are different ways of formulating what constitutes a risk to CI, but overall they have always been associated with physical threats and natural disasters. Both natural and human-induced (intentional or unintentional) incidents may pose risks to CI; in addition, as we have become more and more reliant on technology in our CI sectors, the cyber element has been added.

In 2013 the US Department of Homeland Security (DHS) led the process of formulating the National Infrastructure Protection Plan (NIPP) – *Partnering for Critical Infrastructure Security and Resilience*, which serves as a guide to the national (US) effort to manage risks to critical infrastructure. The NIPP (2013) identifies the three elements of critical infrastructure protection as *Physical*, *Cyber*, and *Human.*

The NIPP-process of protecting critical infrastructure focuses on addressing the three elements, *Physical*, *Cyber*, and *Human*, through a continuous and timely sharing of information, as illustrated in Figure 1 below.

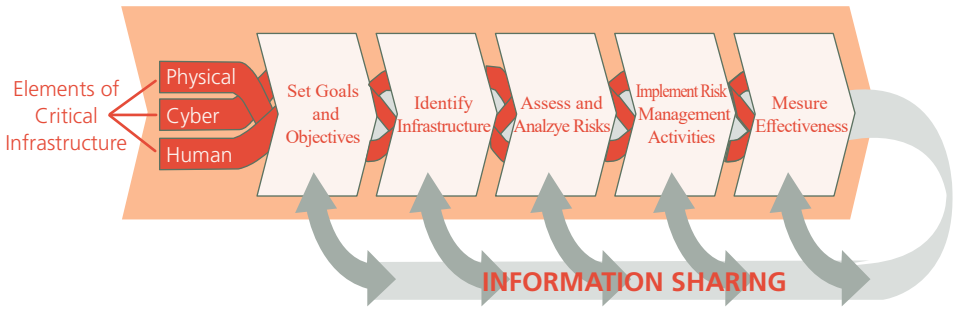

Figure 1: Critical Infrastructure Risk Management Framework (Source: US National Infrastructure Protection Plan (NIPP), Department of Homeland Security (2013))

The process includes setting goals and objectives; identifying infrastructure; assessing and analysing risks; implementing risk management processes, and measuring effectiveness. We will look further into these elements in Section 3 below: Mission Assurance Process.

[2] *Dependencies between countries could, for instance, be within the areas of energy (oil/gas), electric power, or water resources.*

The physical threats described in the NIPP may be either naturally occurring, such as a natural disaster (flooding, heavy snowfall, volcano, earthquake, tsunami etc.) or human-induced. Human-induced threats may be either intentional (a wilful act such as terrorist or other criminal activity) or unintentional (e.g. an accident or security violation). Some threats, such as forest fires, may be either naturally occurring or human-induced.

To mitigate the physical risks and hazards to a CI facility it must not only be located where it is not in direct danger from being destroyed or damaged by natural disasters, but the facility itself must also be well-protected from intentional human-induced activity such as terrorism, and unintentional human-induced activity such as an accident with an impact on the CI facility.

A perimeter fence, 24/7 guarding, CCTV, access control and so on should be in place. A facility such as an Internet Exchange Point (IXP) could also be disguised as just another building in a block, hidden in plain sight.

Just like the physical threats, the threats to CI and CII from cyberspace are human-induced as either intentional (e.g. a cyber-attack) or unintentional (e.g. failing to patch and update an IT system). Although there are other models to consider when focusing on intentional human-induced threats to CI/CII from cyberspace, two models for strengthening cyber-security immediately spring to mind – both with the aim of breaking an intruder's way into the system that is being defended.

The Lockheed Martin Cyber Kill Chain® Model (Lockheed Martin Corporation, 2015) outlines the usual steps in a cyber-attack and includes seven sequential steps for interrupting an attack:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (C2)
7. Actions on Objectives.

As a variation of the Lockheed Martin Cyber Kill Chain® Model, the two-stage SANS Industrial Control System Cyber Kill Chain model (SANS, 2015) focuses on attacks directed towards the Industrial Control System (ICS) in the CI system that is being targeted, rather than the IT systems.

Stage 1 of this model resembles the Lockheed Martin model (albeit with slightly different wording) and deals with Cyber Intrusion Preparation & Execution.

Stage 2 of the SANS ICS model deals with ICS Attack Development & Execution.

The third element described in the NIPP is the human factor. We have described the physical security that may help protect the CI/CII facility against intruders from outside. Another factor is, of course, the insider threat. Although rare, disgruntled employees who have a desire to harm their own company for an ideological, political or financial motive also pose a threat. To minimize such threats procedures should be in place whereby risks are identified, policies are updated, and control is implemented.

The process outlined in the NIPP (Figure 1) may vary from other processes in other nations, as institutions and responsibilities differ from country to country, but the general principle remains the same. Protection of CI and CII is not purely a question of strengthening cyber security – it is also to a large extent about strengthening physical and human security. The questions must be asked, what are you protecting, and what are you protecting against?

The approach to the protection of CI/CII must be holistic so that it is protected against the most dangerous and most likely threats. As an example, you would not have succeeded in protecting your CI/CII by rigorously updating and constantly patching your IT system if your server room is located in a cellar subject to flooding, or in a building with little or no security, or if your employees do not adhere to the security protocol. Best practices for both physical and human security must also be thought into the process.

3 MISSION ASSURANCE PROCESS

To be sure that CI/CII is protected in the best way possible and that the various sectors can still perform their mission, it is necessary to go through a process to strengthen resilience and minimise the risks.

In the UK the Cabinet Office, the National Cyber Security Centre (NCSC), and the Centre for the Protection of National Infrastructure (CPNI) have made a flyer, *Improving our Understanding of Critical National Infrastructure*, in which a five-step Criticalities Assessment is outlined. The five steps are:

1. Map Essential Functions
2. Determine Systems
3. Assess Sector Impacts
4. Identify supporting Systems, Relationships and Organisations
5. Assess Cross-sector Impacts

Essentially, the purpose of the (US) Mission Assurance Process is the same as the UK model – to be able to make a Risk Decision to either mitigate a risk, remediate it, or accept it, if the risk cannot be dealt with.

I have chosen to present the Mission Assurance Process (Figure 2 below) based on an illustration by DISA showing the process described in the (US) Department of Defense Directive 3020.40 of 2016.

Although focused on the US, the directive has some general aspects and the process seems both elaborate and simple and may be universally applied.

The illustration in Figure 2 has been amended to be more generically applicable to countries outside the US, and hopefully will be broad enough to be of direct value for nations wishing to strengthen the protection of their CI/CII.

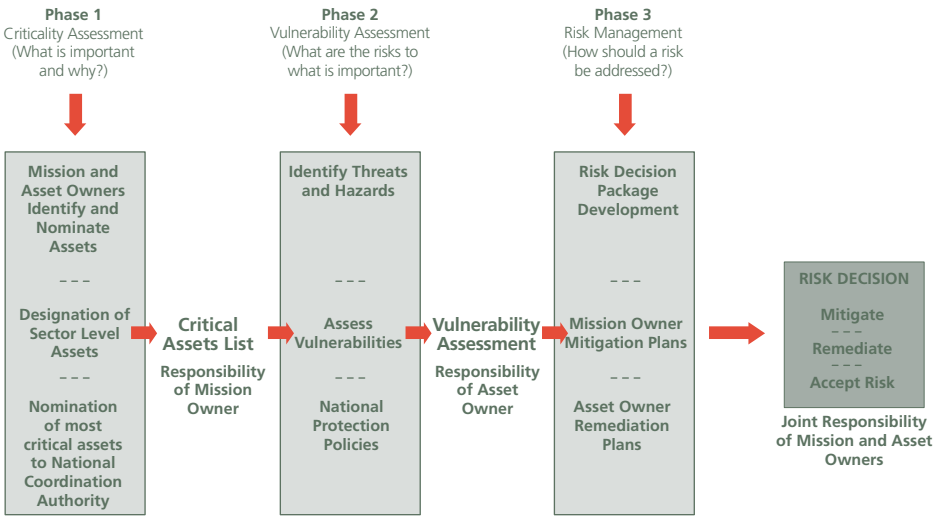

Figure 2: Mission Assurance Process (Source: Based on DISA illustration of US DoD Directive 3020.40 – Mission Assurance)

For much of the CI/CII in our societies, the sector responsible for maintaining a service and those who actually perform it are not the same. The level of privatisation may vary from country to country, but in many cases services have been outsourced to private companies, so the mission owner (sector) and asset owner (company) are not the same.

In **Phase 1** of the Mission Assurance Process, mission owners and asset owners must make a Criticality Assessment determining what is important and why by identifying and nominating assets to a national coordination authority. The mission owner puts these assets on the Critical Assets List.

In **Phase 2** of the process the asset owner will identify threats and hazards by determining what the risks are to what is important and make a Vulnerability Assessment.

In **Phase 3** a plan for Risk Management is formulated by how the risks should be addressed. The mission owner will determine what steps could be taken to mitigate the risk, and the asset owner will plan steps to remediate the hazards.

Based on the outcome of Phases 1-3 a Risk Decision may be formulated to mitigate risks, remediate hazards, or to accept the risk as a condition.

Forming a national coordination authority with all sectors represented and mapping the CI/CII and the interdependencies of different sectors would be a first step (i.e. determining which sectors rely on the services of others).

As illustrated in Figure 3, it would quickly become apparent that most CI sectors have interdependencies with each other and, therefore, there is a great need for cross functional coordination and collaboration. In many instances the sector response to risks are »stovepiped« with not enough coordination between sectors.

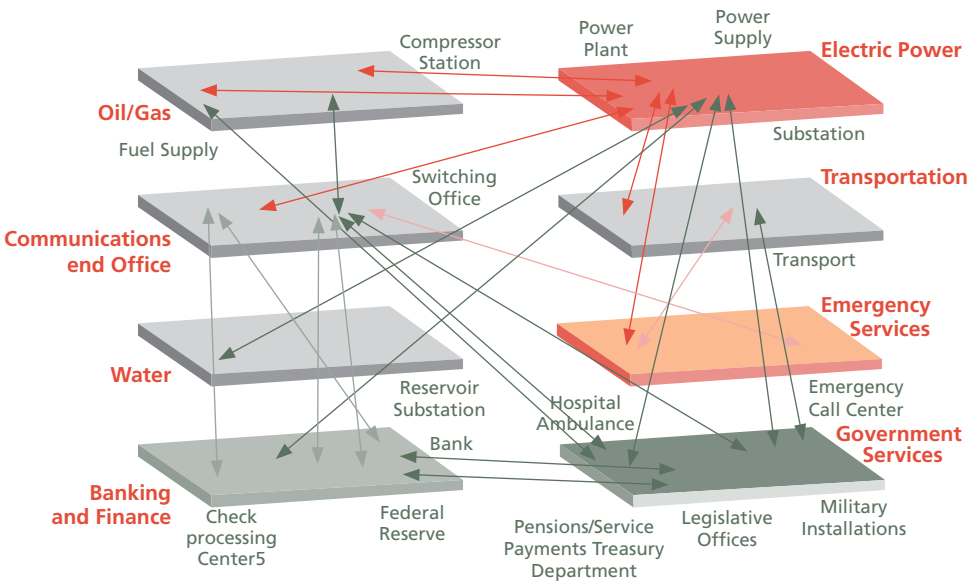

Figure 3: Interdependencies between CI/CII sectors (Source: Ehlen, M. A., Critical Infrastructure Interdependencies, Researchgate.net)

4 COORDINATION, COOPERATION AND PUBLIC PRIVATE PARTNERSHIP

As described in the Mission Assurance Process, CI/CII mission and asset owners need to coordinate their efforts and work closely together. Many of the CI/CII assets and services are today privately owned, whereas the mission owner would normally be a government institution with the responsibility of delivering services within a given sector. For example, a ministry in a country would have overall responsibility for telecommunications, but the services would be provided to the citizens via privately owned and operated telecommunication providers.

In this instance (and examples like it in other CI/CII sectors) there would be a need for close coordination and cooperation between the public and private entities – government agencies and private companies.

According to the European Union Agency for Cybersecurity (ENISA), a »*public-private partnership (PPP) is a long-term agreement/cooperation/collaboration between two or more public and private sectors that has developed through time in many areas*.«

In November 2017 ENISA published *Public Private Partnerships (PPP) Cooperative Models* in which a number of recommendations concerning PPP were brought up:

- Motivation for the private sector to participate should be a priority when establishing a PPP
- The participants should agree to a legal basis when creating a PPP
- Public institutions should lead the PPP or the national action plan for PPP
- PPPs should invest on internal private-private and public-public collaboration
- PPP participants should invest on open communication and a pragmatic approach towards building a PPP
- The representatives of the government should be allowed to participate in the meetings with non-disclosure agreement
- Small and Medium Enterprises (SMEs) should also participate in PPPs

In addition to these points a PPP should form the basis for sharing best practices, as well as actionable information. Furthermore, public entities often have access to information and resources not available to the public, and have the authority to launch criminal investigations and law enforcement actions.

It is also the government which is in a position to regulate areas such as the level of requirement to share information. In many cases private companies would probably be reluctant to publicly state that they have been the victim of, for example, a ransomware attack, as stock prices may be affected. On the other hand sharing such information in a PPP may help to put a stop to such attacks.

A well-functioning PPP is built on trust and dialogue in equal terms, which is why it is important for regulators to base a regulation on, for example, sharing information about cyber-attacks (or other forms of attack) directed against the CI/CII assets (public or private companies), on a shared understanding of the level and speed of information needed to be provided.

An aspect of PPP often overlooked or neglected is exercises. Each year the CCDCOE conducts Locked Shields – a unique international cyber defence exercise offering the most complex technical live-fire challenge in the world. This exercise also makes it possible for the participants to train and exercise PPP within their national teams.

With the goal of enhancing cyber security in the European Union (EU), the European Commission made the first EU-wide legislation, the Network and Information Security (NIS) directive (EU 2016/1148)[3]. As it is an EU directive, EU Member States have begun to adopt national legislation incorporating the content.

The NIS Directive consists of three parts:

National capabilities, whereby EU Member States must have certain national cybersecurity capabilities, e.g. having a national Computer Security Incident Response Team (CSIRT), and carrying out cyber exercises, etc.

Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc.

National supervision of critical sectors such as energy, transport, water, health, digital infrastructure and the finance sector.

The European Commission has now proposed a NIS2 Directive to introduce a common higher level of cyber security in the EU. Among other things the NIS2 Directive would *strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU* (European Parliament, 2021).

It follows from Article 3 of the North Atlantic Treaty that *in order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.*

Even though a (cyber) attack directed against CI/CII in a NATO Member State does not reach the threshold for an armed attack, it still follows the principle of Article 3

[3] *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.*

that each Member Nation should be resilient and take its own precautions to protect its CI/CII.

The NATO Computer Incident Response Capability (NCIRC) is responsible for protecting NATO's own networks and sites (NATO, 2022). In a similar manner the EU Institutions have set up a permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies.

As NATO and the EU face many of the same challenges in cyber security, the two organisations are cooperating by, for instance, increasing their information sharing on cyber incidents. In this context NCIRC and CERT-EU signed a technical arrangement on 10 February 2016.

Ambassador Sorin Ducaru, NATO Assistant Secretary General for Emerging Security Challenges at the time, stated that the *»…agreement facilitates technical information sharing between NCIRC and CERT-EU to improve cyber incident prevention, detection and response in both organisations, in line with their decision-making autonomy and procedures«* (HSD, 2016).

Since then NATO-EU cooperation has increased, and apart from information sharing also covers coordinated planning and concrete cooperation (EU Defence, 2020).

Regardless of whether the cooperation is national in the form of PPP or supranational in the form of NATO-EU cooperation, we, both as individual countries and as NATO and/or EU Member States, stand a better chance of protecting our CI/CII if we coordinate our efforts and cooperate by sharing actionable information.

Conclusion

There is no uniform definition of critical infrastructure (CI) and critical information infrastructure (CII), but CI may be defined as the elements essential for the functioning, integrity and security of a society. Likewise CII may be described as *»…information and communications systems whose maintenance, reliability and safety are essential for the proper functioning of a country. The critical information infrastructure is a part of the critical infrastructure«* (RIA, 2021).

According to the (US) National Infrastructure Protection Plan (NIPP) – *Partnering for Critical Infrastructure Security and Resilience,* the risks to CI/CII may be either *Physical*, *Cyber* or *Human* related, or a combination thereof.

Physical threats may be either natural or human-induced (intentional or unintentional) and protective measures should be implemented to secure the functioning of the CI/CII facility.

The seven-step Lockheed Martin Cyber Kill Chain® Model and the two-stage SANS Industrial Control System (ICS) Cyber Kill Chain may serve to illustrate the cyber threats, and finally, the human threats may take the form of either intentional

or unintentional actions. Although rare, insider threats cannot be discounted and control measures must be implemented and followed by all staff.

No two countries are exactly alike and there is no »one size fits all« solution, but in order to properly protect CI/CII it is necessary to conduct the national variant of the Mission Assurance Process with:

– a Criticality Assessment (what is important and why?);
– a Vulnerability Assessment (what are the risks to what is important?);
– and Risk Management (how should the risk be addressed?)

Based on this, it is possible to make a Risk Decision to either mitigate, remediate, or accept the risk.

Finally, the interdependencies between sectors, as well as the coordination of efforts and cooperation between actors – both nationally in the form of PPP and internationally in organisations such as NATO and the EU – are hugely important. Most countries operate with sector responsibilities, but it will be crucial for success that the interdependencies are well known and efforts are coordinated centrally, with representation from the necessary actors, both public and private.

Bibliography

1. *Assante, M., J., Infrastructure Protection in the Ancient World, 2009, Proceedings of the 42nd Hawaii International Conference on System Sciences. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.401.7316&rep=rep1&type=pdf, 14 March 2022.*
2. *CERT-EU, RFC 2350, Version 5.2, 2022. https://media.cert.europa.eu/static/RFC2350/RFC2350.pdf, 26 March 2022.*
3. *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, Article 2(a), 2008. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG&toc=OJ%3AL%3A2008%3A345%3ATOC, 10 March 2022.*
4. *Ehlen, M. A., Critical Infrastructure Interdependencies, Researchgate.net, 2013. https://www.researchgate.net/figure/Critical-Infrastructure-Interdependencies_fig3_257560357, 15 March 2022.*
5. *ENISA, Critical Information Infrastructures, 2021. https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii?tab=details, 10 March 2022.*
6. *ENISA, NIS Directive. https://www.enisa.europa.eu/topics/nis-directive, 16 March 2022.*
7. *ENISA, Public Private Partnerships (PPP) Cooperative Models, 2017. https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models, 16 March 2022.*
8. *ENISA, Public-Private-Partnership (PPP). https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps, 16 March 2022.*
9. *EU Defence, EU-NATO Cooperation, 2020. https://www.eeas.europa.eu/sites/default/files/eu_nato_factshee_november-2020-v2.pdf, 26 March 2022.*
10. *EUR-Lex, Document 32016L1148, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. https://eur-lex.europa.eu/eli/dir/2016/1148/oj, 16 March 2022.*

11. *European Commission, NATO and CERT-EU Discuss Cyber Threats ahead of EU Elections, 2019. https://ec.europa.eu/info/news/nato-and-cert-eu-discuss-cyber-threats-ahead-eu-elections-2019-may-06_en, 26 March 2022.*
12. *European Parliament, The NIS2 Directive - A High Common Level of Cybersecurity in the EU, 2021. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf, 17 March 2022.*
13. *HSD Securitydelta.nl, NATO and the European Union Enhance Cyber Defence Cooperation, 2016. https://securitydelta.nl/news/newsitem/587-nato-and-the-european-union-enhance-cyber-defence-cooperation, 26 March 2022.*
14. *INSIDER, Photos: How Facebook and Google use sonar ships, gigantic underwater plows, and divers to lay thousands of miles of undersea internet cables around the globe, 2021. https://www.businessinsider.com/google-facebook-giant-undersea-cables-internet-tech-2021-9, 9 March 2022.*
15. *Lockheed Martin Corporation, Seven Ways to Apply the Cyber Kill Chain® with a Threat Intelligence Platform, 2015. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf, 14 March 2022.*
16. *NATO (The North Atlantic Treaty Organization), Cyber Defence, 2022. https://www.nato.int/cps/en/natohq/topics_78170.htm, 23 March 2022.*
17. *RIA - Republic of Estonia Information System Authority, Critical Information Infrastructure Protection CIIP, 2021.https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html, 10 March 2022.*
18. *Ruonavar, F. P., DISA Task Critical Asset Nomination Process, 2018. https://www.disa.mil/-/media/Files/DISA/News/Events/Symposium/1---Rounavar_DISA-Task-Critical-Asset-Nomination-Process_approved-FINAL.ashx, 10 March 2022.*
19. *SANS, The Industrial Control System Cyber Kill Chain, 2015.https://na-production.s3.amazonaws.com/documents/industrial-control-system-cyber-kill-chain-36297.pdf, 14 March 2022.*
20. *The North Atlantic Treaty, 1949. https://www.nato.int/cps/en/natolive/official_texts_17120.htm, 17 March 2022.*
21. *UK Cabinet Office, the National Cyber Security Centre (NCSC), and the Centre for the Protection of National Infrastructure (CPNI), Improving our Understanding of Critical National Infrastructure, 2020. file:///C:/Users/henrik.beckvard/Downloads/CNI%20Criticalities%20KB%20Flyer%20(2).pdf, 14 March 2022.*
22. *UK Centre for the Protection of National Infrastructure (CPNI), Critical National Infrastructure, 2021. https://www.cpni.gov.uk/critical-national-infrastructure-0, 9 March 2022.*
23. *US Department for Homeland Security, National Infrastructure Protection Plan (NIPP) – Partnering for Critical Infrastructure Security and Resilience, 2013, p 15. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf, 11 March 2022.*
24. *US DoD Directive 3020.40, Mission Assurance (MA), 2016. https://irp.fas.org/doddir/dod/d3020_40.pdf, 14 March 2022.*
25. *US Patriot Act, PUBLIC LAW 107–56—OCT. 26, 2001, UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001, P.L. 107-56, §1016(e), 2001. https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf, 10 March 2022.*

e-mail: henrik.beckvard@ccdcoe.org

e-mail: henrik.beckvard@ccdcoe.org

Henrik P. Beckvard je diplomiral iz prava na univerzi v Köbenhavnu in končal šolanje na štabni šoli Canadian Forces College v Torontu. Opravljal je številne štabne funkcije doma in v tujini, leta 2018 pa ga je dansko ministrstvo za obrambo napotilo kot raziskovalca v Sektor za strategijo Natovega Centra odličnosti za kibernetsko obrambo v Talinu v Estoniji. Je vodja skupine v strateški komponenti vaje kibernetske obrambe Locked Shields in vodja tečajev za zaščito kritične informacijske infrastrukture v tem centru odličnosti.

Henrik P. Beckvard holds a Law degree from the University of Copenhagen and is a Staff College graduate from the Canadian Forces College, Toronto. He has served in various staff positions both domestically and abroad, and since 2018 has been seconded from the Danish Ministry of Defence to the Strategy Branch of the NATO CCDCOE in Tallinn, Estonia, where he serves as a researcher. He is a Team Leader for the Strategic Track for Cyber Defence Exercise Locked Shields and serves as the CCDCOE Course Director for Critical Information Infrastructure Protection.