Author(s): Lehto, Martti

Title: Cyber-Attacks Against Critical Infrastructure

Year: 2022

Version: Accepted version (Final draft)

Please cite the original version:

Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure. In M. Lehto, & P. Neittaanmäki (Eds.), Cyber Security : Critical Infrastructure Protection (pp. 3-42). Springer. Computational Methods in Applied Sciences, 56. https://doi.org/10.1007/978-3-030-91293-2_1

Cyber-attacks Against Critical Infrastructure

Martti Lehto

University of Jyväskylä, Jyväskylä, Finland, martti.lehto@jyu.fi

Abstract In the cyber world, the most important threat focuses on critical infrastructure (CI). CI encompasses the structures and functions that are vital to society's uninterrupted functioning. It comprises physical facilities and structures as well as electronic functions and services. Critical infrastructure systems comprise a heterogeneous mixture of dynamic, interactive, and non-linear elements. In recent years, attacks against critical infrastructures, critical information infrastructures and the Internet have become ever more frequent, complex and targeted because perpetrators have become more professional. Attackers can inflict damage or disrupt on physical infrastructure by infiltrating the digital systems that control physical processes, damaging specialized equipment and disrupting vital services without a physical attack. Those threats continue to evolve in complexity and sophistication.

Key words: critical infrastructure, cyber security, systems of systems

1 Introduction

Most countries have a detailed definition regarding their critical infrastructure, including its importance to society, associated threats, its various parts and sectors, and often the continent by which it is safeguarded. The definitions have normally been published in the context of cyber security strategies. In most countries, this definition has evolved over the years to include an ever-broader range of infrastructures. National definitions differ slightly in the criteria used to define the criticality of an infrastructure. Most countries and institutions use crosscutting criteria, which cover all infrastructures in all sectors.

In the USA there are 16 critical national infrastructure sectors (US-GOV, 2001). The United States describes the critical infrastructure as

> the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The nation's critical infrastructure provides the essential services that underpin American society. (DHS, 2020)

In the UK there are 13 Critical national infrastructure sectors. The United Kingdom States describes the critical infrastructure:

> National Infrastructure consists of those facilities, systems, 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 organizations which are not critical to the maintenance of essential services, but which need protection due to the potential dangers they could pose to the public in the event of an emergency (civil nuclear and chemicals sites for example). (GOV.UK, 2017)

According to the definition used by Finland's National Emergency Supply Agency, critical infrastructure consists of devices, services, and IT systems that are so vital to the nation that their failure or destruction would degrade national security, the national economy, general health and safety, and the efficient functioning of the central government. Finland has identified seven vital societal functions and eight critical infrastructure areas. (Laiho, 2020; Kuokkanen, 2020)

According to the EU commission green book

> the critical infrastructure includes those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments. (EC, 2005)

There are a certain number of critical infrastructures in the community, the disruption or destruction of which would have significant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructures (EU, 2008). The goal of the European Programme for Critical Infrastructure Protection (EPCIP) would be to ensure that there are adequate and equal levels of protective security on critical infrastructure, minimal single points of failure and rapid tested recovery arrangements throughout the European Union (EC, 2006).

In general, critical infrastructure describes the physical and cyber systems and assets that are so vital to the nation that their incapacity or destruction would have a debilitating impact on physical or economic security or public health or safety. So, the nation's critical infrastructure provides the essential services that underpin society. Figure 1 illustrates where dependencies and interdependencies exist in a critical infrastructure system, and highlights the existence of dependencies and the inherent and potential complexity of these relationships for infrastructures (Pye and Warren, 2011, p. 196).

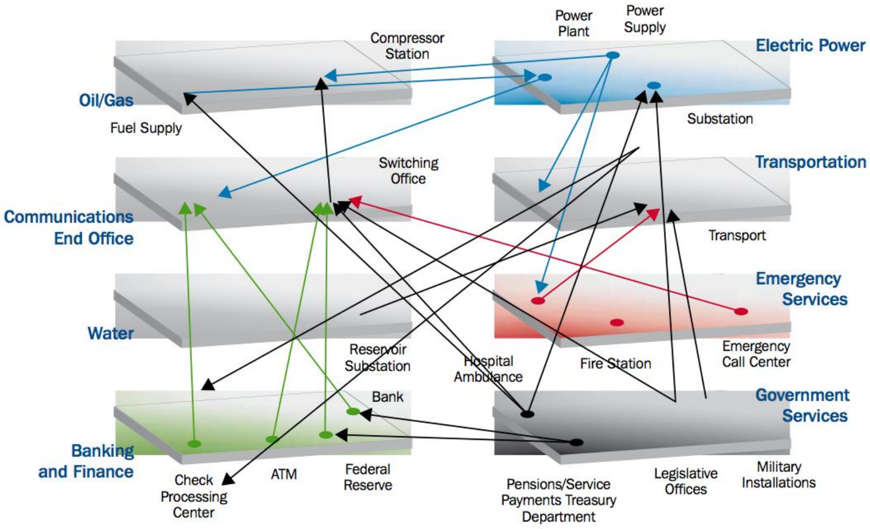

Fig. 1. Critical infrastructure network with its interactions

It is possible to identify three dimensions in safeguarding CI: political, economic, and technical. The political dimension arises from different countries' shared interests in securing their CI systems and the ensuing increased cooperation. The political dimension entails national legislation and national security needs as well as associated international cooperation around these two topics. International cooperation aims to achieve analogous solutions in countries whose needs are comparable. Uniform security legislation and security policies facilitate technical cooperation, especially when several countries have shared infrastructure. The economic dimension affects all companies and business actors which build, own and administer infrastructure systems and installations, and whose operations are driven by economic interests. The economic dimension also includes a fair apportionment of security costs between the stakeholders. The technical dimension encompasses technological advances, including their utilization, and all practical solutions and measures which states, and businesses incorporate in securing the functioning of their critical infrastructure during possible disruptions. (HVK, 2020)

The key aspects of critical national infrastructure issues in cyberspace are the Industrial Control System (ICS), Supervisory Control and Data Acquisition (SCADA) system, Distributed Control System (DCS), and Operational Technology (OT). These systems are key components of infrastructure. Industrial Control System (ICS) is an umbrella term that includes both SCADA and DCS. ICSs are the interfaces where virtual commands generate physical reality in industrial environments. SCADA systems are the software-based elements of those ICSs. ICS and SCADA systems provide real-time, two-way data flow between sensors, workstations, and other networked devices throughout a system. They allow continuous and distributed monitoring and control. DCS is a type of process control system that connects controllers, sensors, operator terminals and actuators.

Operational Technology (OT) encompasses the computing systems that manage industrial operations. These systems likewise support both human-to-machine and machine-to-machine interfaces with industrial processes, often to promote efficiency and automation. Figure 2 illustrates the environment of ICS, SCADA, DCS and OT. (Weed, 2017; Securicon, 2019)

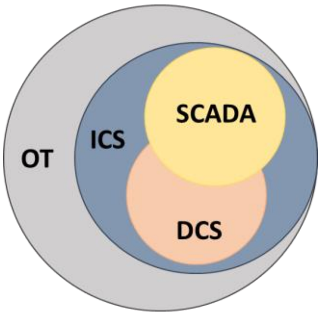

Fig. 2. Environment of ICS, SCADA, DCS and OT (formulated from Securicon (2017))

2 Cyber Security Threats Against Critical Infrastructure

2.1 Motivation of the Attackers

The global community continues to experience an increase in the scale, sophistication, and successful perpetration of cyber-attacks. As the quantity and value of electronic information has increased, so too have the efforts of criminals and other malicious actors who have embraced the Internet as a more anonymous, convenient, and profitable way of carrying out their activities. Of primary concern is the threat of organized cyber-attacks capable of causing debilitating disruptions to a nation's critical infrastructures, functions vital to society, economy, or national security. (Lehto, 2013)

Threats in cyberspace are difficult to define, as it is hard to identify the source of attacks and the motives that drive them, or even to foresee the course of an attack as it unfolds. The identification of cyber threats is further complicated by the difficulty in defining the boundaries between national, international, public, and private interests. Because threats in cyberspace are global in nature and involve rapid technological developments, the struggle to meet them is ever-changing and increasingly complicated. (Lehto, 2013)

For this study, a practical threat taxonomy based on the motivation of the attacker has been developed. The threats included in the suggested threat model are all applicable to the critical infrastructure assets presented in the chapter. The presented threat taxonomy mainly covers cyber-security threats; that is, threats applying to ICT, ICS, and SCADA assets.

One of the most common threat models is a six-fold classification based on motivational factors:

1. Cyber Vandalism,
2. Cybercrime,
3. Cyber Espionage,
4. Cyber Terrorism,
5. Cyber Sabotage, and
6. Cyber Warfare.

With a typology such as these motives can be reduced to their very essence:

1. Egoism,
2. Anarchy,
3. Money,
4. Destruction,
5. Paralysis, and
6. Power.

This six-fold model is modified from Dunn Cavelty's structural model (Dunn Cavelty, 2010; Ashenden, 2011).

Level 1: Cyber vandalism

Cyber vandalism encompasses cyber anarchy, hacking and hacktivism. Hackers find interfering with computer systems an enjoyable challenge. Hacktivists wish to attack companies for political or ideological motives. It is the act of damaging someone's data from the computer that in a way disrupts the victim's business or image due to editing the data into something invasive, embarrassing, or absurd.

Level 2: Cybercrime

Cyber criminals are interested in making money through fraud or from the sale of valuable information. The Commission of the European Communities defines cybercrime as "criminal acts committed using electronic communications networks and information systems or against such networks and systems" (EC, 2007).

According to the Commission, cybercrime can be divided into three categories of criminal activities:

1. Traditional forms of crime committed over electronic communication networks and information systems, such as harassment, threats, or fraud;
2. The publication of illegal content over electronic media, e.g., child sexual abuse material or incitement to racial hatred;
3. Crimes unique to electronic networks, e.g., network attacks, denial-of-service attacks, and hacking.

Cybercrime is a crime in which a computer or smart device is the object of a crime and/or is used to commit a crime. A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable the device.

Level 3: Cyber espionage
Intelligence services are interested in gaining an economic, military, or political advantage for their companies, organizations or countries. So, cyber espionage can be defined as an action aimed at obtaining secret information (sensitive, proprietary, or classified) from individuals, competitors, groups, governments, and adversaries for the purpose of accruing political, military, or economic gain by employing illicit techniques on the Internet, networks, programs, or computers. (Liaropoulos, 2010)

Level 4: Cyber terrorism
Cyber terrorism utilizes networks in attacks against critical infrastructure systems and their controls (Beggs, 2006). The purpose of the attacks is to cause damage and raise fear among the public, and to force the political leadership to give into the terrorists' demands. Although cyber terrorist attacks have not yet materialized, an increased level of "know-how" will arguably make them more likely to occur (UN, 2018).

Level 5: Cyber sabotage
It is an activity in which an attacker (a state actor or a state sponsored group) operating below the threshold of war or executing Military Operations Other Than War (MOOTW). The goals may be to cause instability in the target country, to test one's own offensive cyber-attack capabilities, to prepare for hybrid operations, or to prepare warfare actions. An example is the Stuxnet operation. Stuxnet was a malicious computer worm, which was targeted supervisory control and data acquisition (SCADA) systems and caused substantial damage to the nuclear program of Iran. (Zetter, 2015; US-Army, 1995)

Level 6: Cyber warfare
No universally accepted definition for cyber warfare exists; it is quite liberally being used to describe the operations of state-actors in cyberspace. It is typically defined as an act of war using internet-enabled technology to perform an attack on a nation's digital infrastructure (civilian or military). Cyber warfare per se, requires a state of war between states, with cyber operations being but a part of other military operations (air, land, naval, space).

During the Russo-Georgian War, a series of cyber-attacks swamped and disabled websites of numerous South Ossetian, Georgian, Russian, and Azerbaijani organizations. The attacks were initiated three weeks before the shooting war began in what is regarded as the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains. (Hollis, 2011)

Cyber threats can be categorized based on the attacker's skills as follows (Abomhara and Køien, 2015):

- Unstructured threats consisting of individuals with low or moderate skills who use easily available hacking tools;

- Structured threats by people who know system vulnerabilities and can understand, develop, and exploit codes and scripts (cyber weapons).

2.2 Vulnerabilities

According to the Department of Homeland Security the risk environment affecting critical infrastructure is complex and uncertain, so

> Growing interdependencies across critical infrastructure systems, particularly reliance on information and communications technologies, have increased the potential vulnerabilities to cyber threats and potential consequences resulting from the compromise of underlying systems or networks. In an increasingly interconnected world, where critical infrastructure crosses national borders and global supply chains, the potential impacts increase with these interdependencies and the ability of a diverse set of threats to exploit them. (DHS, 2013)

Implementing ICS/DCS/SCADA-based cyber-physical systems into critical infrastructures brings benefits and also introduces a new set of vulnerabilities and risks to system operators and society.

Threat, vulnerability, and risk form an intertwined entirety in the cyber world. First, there is a valuable physical object, competence or some other immaterial right which needs protection and safeguarding. A threat is a harmful cyber event which may occur. The numeric value of the threat represents its degree of probability. Vulnerability can be defined as an "exploitable weakness or deficiencies in a system, device or its design that allow threat agents/actors to execute commands, access unauthorized data, and/or conduct Distributed Denial of Service (DDoS) attacks" (Bertino et al., 2010). Vulnerabilities may be the outcome of a weakness in system security procedures, software applications, policies and procedures and regulatory compliance. Vulnerability is the inherent weakness in the system which increases the probability of an occurrence or exacerbates its consequences.

Vulnerabilities can be divided into those that exist in (Lehto, 2015)

- People's actions,
- Processes, or
- Technologies.

People like to click all the links.

Very often cybersecurity threats are due to employee errors. The Kaspersky Lab's report says that employee errors accounted for 90% of the data breaches that occurred in the cloud environment. Employees are often victims of social engineering tactics. (Hess, 2019) So, quite often human actors are the weakest link in cybersecurity.

Processes are key to the implementation of an effective cyber security strategy. Processes are crucial in defining how the organization's activities, roles and documentation are used to mitigate the risks to the organization's information. Process vulnerabilities among others lack written security policy, poor regulating policy, lack of security awareness and training, and poor adherence to security, lack of access control and non-existence of disaster/contingency plan.

The main goal of the cybersecurity process is to protect and preserve the confidentiality, integrity, and availability of organizational information assets (Hess, 2019). But processes are nothing if people do not follow them correctly. (FCC, 2014)

Technology solutions protect against cyber risks that may arise from network vulnerabilities but technology itself contains vulnerabilities (HW and SW). So, technological vulnerabilities are security holes in a system.

A software vulnerability is a bug in program coding, configuration, or management. A program can be an algorithm, application, operating system, or browser and control software like communication protocols and devices drives. Hackers use vulnerabilities in software attacks to force systems to give them access to unauthorized data, execute malicious code, obtain remote control, or cause the system to spread infections. The CyLab Sustainable Computing Consortium at Carnegie Mello University estimates that "commercial software has 20-30 code bugs for every 1000 lines of code" (Chong, 2013). Applied Visions, Inc. estimates that 111 billion lines of new software code containing billions of vulnerabilities are coded every year. (Chong, 2013)

A hardware vulnerability is an exploitable weakness in a computer system that enables attack through remote or physical access to system hardware. Hardware vulnerabilities are very difficult to identify. In January 2018, the entire computer industry was put on alert by two new processor vulnerabilities dubbed Meltdown and Spectre that defeated the fundamental OS security boundaries separating kernel and user space memory. The flaws stemmed from a performance feature of modern CPUs known as speculative execution. (Constantin, 2021)

The hardware vulnerabilities are:

- Semiconductor doping: the process of adding impurities to silicon-based semiconductors to change or control their electrical properties,
- Manufacturing backdoors for malware or other penetrative purposes including embedded Radio-Frequency Identification (RFID) chips and memory,
- Manufacturing backdoors for bypassing normal authentication systems,
- Eavesdropping by gaining access to protected memory without opening other hardware,
- Hardware modification with invasive procedures, appliances, or jailbroken software,
- Counterfeiting product,
- Hardware side-channel attacks.

Since vulnerabilities can occur anywhere within the network, deploying a single-point solution will expose the system to numerous threats of attack. Solutions that can be integrated and automated into the security framework to provide distributed protection across the network are the best protection against attacks.

General vulnerabilities relate to areas that communally affect all ICT systems (i.e., individual privacy and personal data, and publicly accessible devices). This also includes vulnerabilities in commercially available mainstream IT products and systems. General vulnerabilities are also in wireless and cellular communication. For example, inadequate security protocols, inadequate authentication mechanisms, energy constrain, poor security and unreliable communication. (ENISA, 2015)

Each critical infrastructure contains specific vulnerabilities in ICS/SCADA systems. The primary causes of ICS and SCADA vulnerabilities fall into three general categories: insecure design, the human element, and configuration issues. An insecure design approach failed to consider the contested, interdependent, and complex environment in which these systems would operate. Poorly or negligently configured equipment provide opportunities for attackers to compromise systems that otherwise would have been secure. (Weed, 2017)

2.3 Attack Vectors

In cybersecurity, an attack vector is a path or means by which an attacker can gain unauthorized access to a computer, network, or information infrastructure to deliver a payload or malicious outcome. Attack vectors allow attackers to exploit system vulnerabilities, install different types of malware and launch cyber-attacks. There are also many different attack vectors that attackers can effectively exploit to gain unauthorized access to IT infrastructure. (Tunggal, 2020)

There is two major types of cyber-attack, non-targeted and targeted attacks. Non-targeted attacks are cyber-attacks that target a wide variety of targets. For example, these attacks include ransomware campaigns and non-targeted malware infections. In un-targeted attacks, attackers indiscriminately target as many devices, services, or users as possible. They do not care about who the victim is as there will be several machines or services with vulnerabilities. To do this, they use techniques that take advantage of the openness of the Internet, which include port scanning, phishing, water holing, ransomware, scanning and other malware infections. (GOV.UK, 2019; Kovanen et.al, 2018)

Targeted attacks are focused on a specific target and the attack campaign requires resources, such as skill and time. This type of threat is often known as Advanced Persistent Threat (APT). Targeted attacks that have been seen so far are focused on espionage or sabotage without destroying any infrastructure. Advancements in attack techniques show that attacks are evolving and reaching the finesse seen in attacks focusing traditional IT networks. Traditional security measures are not enough to counter these attacks as the adversary has time and skills to bypass them. Having a strong and diverse defense in action makes these attacks more time consuming and increase the probability of detection before the adversary's goal is reached. (GOV.UK, 2019; Kovanen et.al, 2018)

A cyber-attack on critical infrastructure occurs when a hacker gains access to a computer system that operates equipment in a manufacturing plant, oil pipeline, a refinery, an electric generating plant, or the like and can control the operations of that equipment to damage those assets or other property. Cyber-attacks may aim to cause disruption in the production system, resulting in unanticipated downtime, wasted production efforts, and/or ruined equipment. (Scheuermann, 2017)

Cyber threats vary but may include, for example, attacks that (UN, 2018)

- Manipulate systems or data such as malware that exploits vulnerabilities in computer software and hardware components necessary for the operation of CIs,
- Shut down crucial systems such as DDoS attacks,
- Limit access to crucial systems or information such as through ransomware attacks.

In a targeted attack an organization is targeted because the attacker has a specific interest in the business or has been paid to target a specific organization. The groundwork for the attack could take months so that they can find the best route to deliver their exploit directly to systems (or users). A targeted attack is often more damaging than an un-targeted attack because it has been specifically tailored to attack organizations systems, processes, or personnel, in the office and sometimes at home. Targeted attacks may include spear-phishing, deploying a botnet, subverting the supply chain. (GOV.UK, 2019)

In general, attack vectors can be split into passive or active attacks:

- Passive: attempts to gain access or make use of information from the system but does not affect system resources, such as typosquatting, phishing and other social engineering-based attacks;
- Active: attempts to alter a system or affect its operation such as malware, exploiting unpatched vulnerabilities, email spoofing, man-in-the-middle attacks, domain hijacking and ransomware.

The most common attack vectors of cyber-attacks are among others (Tunggal, 2020):

- Compromised credentials,
- Weak and stolen credentials,
- Using malicious insiders,
- Missing or poor encryption,
- Misconfiguration,
- Ransomware,
- Phishing and other social engineering-based attacks,
- Exploit unpatched vulnerabilities,
- Brute force attack,
- Spoofing,
- Distributed Denial of Service (DDoS),
- SQL injections,
- Trojans,
- Cross-site scripting (XSS),
- Session hijacking,

- Man-in-the-middle attacks,
- Third and fourth-party vendors.

A typical attack works like this: The cyber attacker starts by establishing a beachhead on the endpoint of the organization that they are aiming to breach. After gaining initial access and establishing persistence, the attacker escalates privileges to gain access to another system that brings them one step closer to their target. From there, the attacker can continue to move laterally until the target is reached, data is stolen, and operations are disrupted – or completely taken over. Cyber operations or attack vectors themselves do not tell about the attacker's motives and goals. For example, hacking and DDos-attacks can be used by all 1-6 level actors. (Orr, 2020)

Example 1. Russian government cyber threat actors have been targeting the U.S. critical infrastructure sectors since at least March 2016 in a coordinated campaign of malware attacks, collectively named Dragonfly. The threat actors used a combination of spear-phishing (highly targeted emails with malicious attachments) and watering hole attacks (introducing malware through well-known industry trade publications' websites) to collect user credentials. The threat actors were able to establish footholds in the target networks and conduct network reconnaissance, move laterally, and collect information pertaining to ICSs. (CISA, 2019)

Example 2 (Hatman, also known as TRITON and TRISIS). This attack platform targets safety controllers manufactured by a major international ICS provider. Safety controllers play an essential role in ICS environments to ensure the safe and predictable shutdown of operational equipment. Hatman malware was specifically designed to allow changes to the safety controller to introduce new functionality that would likely degrade the safety controller's ability to shut down equipment safely. (CISA, 2019)

3 Cyber-attacks Against Critical Infrastructure

Critical infrastructure can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents, or computer hacking, criminal activity and malicious behaviour (EC, 2005). National critical infrastructure could be targeted by hostile states, cyber criminals, terrorists, or criminals for the purposes of disruption, espionage and/or financial gain. In this chapter, the critical infrastructure taxonomy is based on the US taxonomy, in which the government facilities sector and the commercial facilities sector are combined, and the new sector is governmental institutions sector.

3.1 Chemical Sector

The chemical sector manufactures, stores, uses, and transports potentially dangerous chemicals. Chemical sector facilities typically belong in four key functional areas: manufacturing plants, transport systems, warehousing and storage systems, and chemical end users. Most chemical companies have internet-connected devices as part of their process control systems.

For the chemical sector, major cybersecurity issues include impacts to both IT and operational technology (OT) systems and operations due to targeted or opportunistic attacks (e.g., advanced persistent threat, distributed denial of service, or malware and ransomware), disruptions of cloud-based services, or the manipulation of industrial control systems. The sector is vulnerable to the threat of malicious actors physically or remotely manipulating network-based systems designed to control chemical manufacturing processes or process safety systems. (DHS, 2014; CISA, 2019)

Example 3. A notable attack, 'Nitro', occurred in 2011 whereby hackers used a malware called 'PoisonIvy' to steal sensitive data and information from several chemical companies throughout the U.S. (Brenner, 2011)

Example 4. In 2017, a petrochemical facility in Saudi Arabia was attacked using Hatman. The sophisticated attack was intended to sabotage the facility's operations such that safety controls would fail, triggering an explosion. Though the attack was unsuccessful in causing an explosion or hazmat release (owing to an error in the code), the incident demonstrated how similar cyber-attacks may be used to cause physical destruction to critical infrastructure. (CISA, 2019)

Example 5. Hexion, Momentive, and Norsk Hydro all hit by ransomware cyber-attacks. Those chemical manufacturing companies based in Norway and the US have fallen victim to ransomware attacks, after a program called LockerGoga gained access to systems, encrypted files, and disrupted operations. On 19 March 2019, the global aluminum producer Norsk Hydro was forced to shut down its plants and its worldwide network after a security breach blocked access to files and changed the passwords to user accounts across several of its corporate and production control systems. The malware issued a ransom note stating that files had been encrypted and demanding payments in bitcoin to restore access to data. (Stoye, 2019)

3.2 Commercial and Government Facilities Sector

The commercial facilities sector includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging. Facilities within this sector operate on the principle of open public access, meaning that the public can congregate and move freely without highly visible security barriers. Most of these facilities are privately owned and operated. Sector operates on the principle of open public access, meaning that the public can move freely throughout these facilities without the deterrent of highly visible security barriers. (DHS, 2014; DHS, 2016)

The government facilities sector includes a wide variety of buildings. Many government facilities are open to the public while others are not. These facilities include general-use office buildings and special-use military installations, embassies, courthouses, national laboratories, and structures that may house critical equipment, systems, networks, and functions. (DHS, 2014) The education facilities subsector encompasses early childhood, pre-primary, basic, upper secondary, vocational, and higher education facilities (public, and private).

Cyber intrusions into automated security and supervisory control and data acquisition systems are risks. The increasing reliance on automated security systems and automated building management systems will likely increase vulnerabilities and the likelihood of cyber intrusion, especially in the form of sabotage by current or former insiders with malicious intent. Cyber intrusion into the security systems of government facilities could compromise the protection of facilities, civil servants, and the public and allow for exploitation and attacks with significant consequences. (DHS, 2014)

Higher education institutions often collect and store sensitive, personal student data and databases (identity numbers, health, financial, and educational data). Disruptions to institutional data systems could impact the capacity to effectively perform essential business operations and could cause a temporary to long-term school closure. Although a cyber-attack on an education facility would not likely impose cascading effects for the nation, it can have such effects on the campus community through the compromising of personal data, security systems, and research facilities that rely on cyber elements or of emergency management data housed electronically. (DHS, 2014)

Example 6. In 2011, two research labs, Pacific Northwest National Laboratory (PNNL) and Thomas Jefferson National Laboratory in Newport News, Virginia were victims of a cyber-attacks. The attacks eventually caused these labs to shut down all internet access and website access for a couple days. (Finkle, 2011)

3.3 Communications Sector

The communications sector is an integral component of the economy, underlying the operations of all businesses, public safety organizations, and government. The communications sector is comprised of telecommunications, internet, postal services, and broadcast. The sector provides services in terrestrial, satellite, and wireless transmission systems. The transmission of these services has become extremely interconnected; satellite, wireless, and wireline providers depend on each other to carry and terminate their traffic, and companies routinely share facilities and technology to ensure interoperability and efficiency. The private sector owns and operates the majority of communications infrastructure. (DHS, 2014; GOV.UK, 2017)

The telecommunication industry has always been an integral part of every aspect whether it is related to the business or individuals, providing a variety of services that connect and communicate with millions of people worldwide. In recent years, the industry has experienced a fundamental transformation with the developments of network technologies. Today's threats are a realization of traditional IP based threats within the all-IP 4G network combined with insecure legacy 2/3G generations. Moving into the 5G era, the threat landscape will increase due to the new services and technologies being introduced. (Kumar, 2020; GSMA, 2019)

The sector builds and operates complex networks and stores voluminous amounts of sensitive data associated with individuals and corporations. These are among the reasons that make this field more lucrative to malicious actors or hackers. Over the years, the security vulnerabilities of telecom devices have been increased dramatically and now equipping a major space of the threat landscape. (Kumar, 2020)

Cyber disruptions of communications systems present unique challenges due to global connectivity. The exploitation of vulnerabilities around the world can begin affecting critical communications components in a matter of minutes. A successful cyber-attack on a telecommunications operator could disrupt service for thousands of phone customers, sever Internet service for millions of consumers, cripple businesses, and shut down government operations. Malicious actors may pose many risks, which can impact data, networks, and components, which create financial losses for organizations and severe disruptions in the operations of organizations. (DHS, 2014; Lobel, 2014)

CrowdStrike published its 2020 Global Threat Report (CrowdStrike, 2020) which shows that the telecommunications and government sectors were the most targeted by the threat groups monitored by the cybersecurity firm. In the case of the telecom sector, many of the attacks were attributed to China-linked hacker groups (Kovacs, 2020).

DDoS (Distributed Denial of Service) attack is one of the most common types of direct cyber-attacks that can make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. The telecom industry experiences more DDoS attacks than any other industry. These attacks can condense network capacity, swell traffic costs, disrupt the availability of service, and even compromise internet access by hitting ISPs. (Kumar, 2020)

Other threats that exist are the exploitation of vulnerabilities in network and consumer devices, attacks against supply chain, cloud services, IoT environment, and compromising subscribers with social engineering, phishing, or malware. Growing numbers of cyber attackers now combine data sets from different sources, including open sources, to build up detailed pictures of potential targets for blackmail and social engineering purposes. Insiders from cellular service providers are recruited mainly to provide access to data, while staff working for Internet service providers are chosen to support network mapping and man-in-the-middle attacks. Also aging protocols are a significant vulnerability. (Kaspersky, 2016; GSMA, 2019)

Example 7. The 2016 Dyn cyber-attack was a series of DDoS attacks on October 21, 2016, targeting systems operated by Domain Name System (DNS) provider Dyn. The attack caused major Internet platforms and services to be unavailable to large swathes of users in Europe and North America. The Mirai worm affected 100,000 UK Post Office broadband customers and 900,000 customers of Deutsche Telecom and was used to mount a DDoS attack, which in turn resulted in outages across Twitter, Spotify, Netflix, Paypal and other services. (Wikipedia)

Example 8. In 2018 hackers infected more than 500,000 routers with malware that could cut off internet access and steal login credentials. The hackers have the power to simultaneously kill the devices and take down the internet for vast numbers of people as a result. The hackers have installed a malware known as VPNFilter on all those routers from a range of vendors, including Linksys, MikroTik, Netgear and TP-Link, which had publicly known vulnerabilities. Victims were spread across a total of 54 countries, but most of the targets were based in the Ukraine. (Goodin, 2018)

3.4 Critical Manufacturing Sector

The critical manufacturing sector is crucial to economic prosperity and continuity. This sector has identified the following industries to serve as the core of the sector (DHS, 2014):

- Primary Metal Manufacturing,
- Machinery Manufacturing,
- Electrical Equipment, Appliance, and Component Manufacturing,
- Transportation Equipment Manufacturing.

Cyberthreats against manufacturing sector focus among others compromised on-site or remote ICS and SCADA systems. Manipulation of these systems can paralyze individual equipment or systems as well as entire production lines. Supply chain systems are vulnerable because of increased reliance on advanced information technology (IT) systems. State-sponsored and other actors could potentially defeat competition and / or obtain competitive secrets through cyber-intrusion. (DHS, 2014)

Example 9. SHAMOON virus directed against Saudi Arabian Oil Company (ARAMCO) in 2012. The virus spread throughout the company's network and affected as many as 30,000 computers. Without a way to pay them, gasoline tank trucks seeking refills had to be turned away. Saudi Aramco's ability to supply 10% of the world's oil was suddenly at risk. In addition to affecting ARAMCO, the virus spread and was found on the system of RasGas, a Qatari owned liquefied natural gas company. (Pagliery, 2015; Pagliery, 2016; 2014; Ballou et.al, 2016)

Example 10. In November 2014, in the hack of a German steel mill, the attackers targeted emails using a ‘spear phishing’ technique to obtain log-in information, which gave them access to critical production systems at the mill, leading to massive damage. (Spiegel, 2014)

Example 11. In November 2016, hackers destroyed thousands of computers at six Saudi Arabian organizations, including those in the energy, manufacturing, and aviation industries. The attack was aimed at stealing data and planting viruses; it also wiped the computers, so they were unable to reboot. Hackers used a version of a specific type of cyberweapon, which operates like a time bomb. (Pagliery, 2016)

3.5 Dams Sector

The dams sector is comprised of assets that include dam projects, hydropower generation facilities, navigation locks, levees, dikes, hurricane barriers, mine tailings, industrial waste impoundments, and other similar water retention and water control facilities. These dams, locks, pumping plants, canals, and levees provide water supply, power generation, navigable waterways, flood protection, and unique environmental stability and enhancements to habitats across the country. (DHS, 2014; DHS, 2015)

The increasing use of standardized industrial control systems technology increases the sector’s potential vulnerability to direct cyber-attacks and intrusions, which are a constant potential threat across the dam system environment. Opening the flood gates by cyber-attack can cause significant damage, and, if hydropower governors are cyber vulnerable, then generators and turbines could be destroyed in a cyber-attack. In 2016 the US ICS-CERT performed 98 assessments and recorded 94 instances of weak boundary protection of the control system which could facilitate unauthorized access. There were also incidences of unnecessary services, devices, and ports on control systems, as well as weak identification and authentication management. (DHS, 2014; WaterPower, 2019)

Example 12. In 2013, Iranian attackers were accused of infiltrating a dam in New York and stealing information from the energy company Calpine Corp. The small dam is not built for energy production purposes but to control water levels. The system was directly connected to the Internet and there was no need for the attacker to go past business network nor DMZ. The automation system of controlling the operation of the gate was not active and therefore it is not possible to evaluate the adversary's capabilities regarding the control system because it could not have been operated remotely. (AP, 2015)

Example 13. In 2016, an Iranian nation-state committed a cyber-attack against the United States at the Rye Brook Dam in New York. The hackers accessed industrial control systems within the dam but were fortunately unable to release the water behind the dam due to scheduled maintenance. However, this could have been a disaster waiting to happen with just a few clicks. (Thompson, 2016)

3.6 Defense Industrial Base Sector

The Defense Industrial Base (DIB) is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, components, and parts. The DIB sector has become heavily dependent on IT infrastructure, operating within an increasingly information-driven environment. DIB sector IT infrastructure is vulnerable to denial-of-service attacks, data theft and malicious modification of information. These vulnerabilities contribute greatly to the risk in the sector. Foreign entities and non-state actors seek to acquire access to sensitive and classified DIB sector information and technologies by expanding their cyber intelligence/espionage activities. (DHS, 2014)

In cyber-attacks, foreign actors are stealing large amounts of sensitive data, trade secrets, and intellectual property (IP) every day from DIB firms. This comes in many forms (e.g., insider threat, phishing). The biggest issue confronting the DIB is how information security is being implemented, i.e., system users not following procedures or system administrators not applying fixes to known vulnerabilities. The DIB relies on commercial-off-the-shelf (COTS) information system products that are often flawed in their design and implementation, thus offering a host of vulnerabilities to those who would exploit them. (Biancuzzo, 2017; DHS, 2010a)

Cyber-attacks designed to steal IP from the unclassified networks of companies have increased. The small firms are particularly vulnerable because they have challenges to aquire the costly cybersecurity tools (CSTs) and skilled professionals required to adequately protect their networks. In addition, ransomware attacks, possibly by different perpetrators, have also recently increased and have resulted in the destruction of data held on the unclassified networks of small companies and local governments. (Gonzales et al., 2020)

The Defense Industrial Base is always under constant ransomware attacks. The malicious actors behind these attacks often block access to sensitive government data, intellectual property, and even trade secrets until they get paid. This can potentially harm a government's military capabilities and operations. DIB networks host critical operational assets and data that is crucial to national security. If the systems get breached, national security will be compromised. (Mallon, 2020)

Example 14. In 2007 Chinese hackers stole technical documents related to the data on the F-35 Joint Strike Fighter, the F-22 Raptor fighter jet, and the MV-22 Osprey. This espionage reduced the adversaries' costs and accelerated their weapon systems development programs, enabled reverse-engineering and countermeasures development, and undermined the U.S. military, technological, and commercial advantage. (US-GOV, 2019)

3.7 Emergency Services Sector

The Emergency Services Sector (ESS) is a community of emergency personnel, along with the physical and cyber security resources, providing a wide range of preparedness and recovery services during both day-to-day operations and incident response. ESS is comprised of the following disciplines (DHS, 2014; Loukas et.al, 2013):

- Law Enforcement: Maintaining law and order and protecting the public from harm.
- Fire and Rescue Services: Prevention and minimizing loss of life and property during incidents resulting from fire, medical emergencies, and other all-hazards events.
- Emergency and Medical Services (EMS): Providing emergency medical assessment and treatment at the scene of an incident, during an infectious disease outbreak, or during transport and delivery of injured or ill-individuals to a treatment facility as part of an organized EMS system.
- Emergency Management: Leading efforts to mitigate, prepare for, respond to, and recover from all types of multijurisdictional incidents. Emergency management increasingly depends on computational and communication systems for coordination, communication, information gathering, training, and planning.
- Public Works: Providing essential emergency functions, such as assessing damage to buildings, roads, and bridges; clearing, removing, and disposing of debris; restoring utility services; and managing emergency traffic.

Through partnerships with public and private sector entities, ESS's mission is to save lives, protect property and the environment, assist communities impacted by disasters (natural or manmade), and aid recovery from emergency situations. (DHS, 2014; DHS, 2012)

Cyber targeting of the ESS will likely increase as systems and networks become more interconnected and the ESS becomes more dependent on information technology for daily operations. For example, cyber disruption of communications systems, computer networks in service vehicles, or GPS during an emergency operation could dramatically disrupt or delay the initial response to an event. (DHS, 2014)

Many ESS activities, such as emergency operations communications, database management, biometric activities, telecommunications, and electronic systems (e.g., security systems), are conducted by partners virtually. These activities are vulnerable to cyber-attack. Additionally, the Internet is widely used by the sector to provide information as well as alerts, warnings, and threats relevant to the ESS. (DHS, 2010b; Jones, 2017)

The following risks and impacts may occur in the ESS because of cyber-attacks (DHS, 2012):

- Compromised ESS database causes disruption of mission capability or corruption of critical information,
- Public alerting and warning system disseminates inaccurate information,
- Loss of communications lines results in disrupted communications capabilities,
- Closed-circuit television (CCTV) jamming/blocking results in disrupted surveillance capabilities,
- Loss of communications lines results in disrupted communications capabilities for ESS troops,
- The DDoS attack against services of public safety and emergency services communications networks may lead to a paralysis of the services and loss of life.

Example 15. DDoS attacks are often used as a form of protest. After officer-involved shootings in 2014 in Denver and Albuquerque, divisions of Anonymous launched DDoS attacks to shut down the online service of both police departments. (Police1, 2017)

Example 16. In December 2016, a law enforcement agency near Dallas, was the victim of a ransomware attack when an employee clicked on a link in a phishing email that appeared to be from another law enforcement agency. The agency lost a substantial number of digital files, including video evidence. (Quinn, 2018)

Example 17. On March 22, 2018, a ransomware attack encrypted data on the City of Atlanta's government servers, affecting various internal and customer applications, including those of the Atlanta Police Department. During the same month, the City of Baltimore, Maryland, had its dispatch system taken offline for more than 17 hours due to a cyber-attack. (Quinn, 2018)

3.8 Energy Sector

The energy sector is usually divided into three interrelated segments: electricity, petroleum, and natural gas. Electricity infrastructure is highly automated and controlled by utilities and regional grid operators that rely on sophisticated digital energy management systems. The modern electric grid is dependent upon cyber-physical systems, engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components. Also, oil and natural gas infrastructure is highly automated and controlled by pipeline operators, terminal owners, and natural gas utilities that rely on digital sophisticated energy management systems. (DHS, 2014; INL, 2016; EECSP, 2017)

The energy infrastructure is arguably among one of the most complex and critical infrastructures since other sectors depend upon it to deliver their essential services.

The energy industry is an IP-intensive industry, meaning it holds massive intellectual property. The energy sector consists of all the industries involved in the processes of energy production, distribution, and transmission. ICSs are used for controlling these processes. Energy infrastructures have turned into highly distributed systems, which require proactive protection. (DHS, 2014; INL, 2016; EECSP, 2017)

Mainly for that reason, it is an attractive target for cyber criminals and cyber espionage. Cyber espionage against the energy sector may be rooted in political and economic motives, which may give the actor access to knowledge that presents a technological advantage, constituting a potential threat to the energy security. (Macola, 2020)

Attacks on ICS of the energy sector have become more targeted than in the past. Attackers have become more knowledgeable about how to go after industrial control systems, using attacks customized to exploit ICS. Additionally, threat actors are paying close attention not only to payload, but delivery as well, focusing on ICS trusted relationships.

The power system has evolved into an ICS-enabled industry that increasingly relies on intelligent electronic devices (IEDs) using bidirectional communication to execute operations. Assets may be vulnerable if an infrastructure's industrial control systems are connected to the Internet, either directly or indirectly. For example, control system networks may be connected to the corporate business network, which, in turn, is connected to the Internet. These connections increase the network's vulnerability to direct cyber-attacks that could potentially disrupt movement and increase risk to the sector. (DHS, 2014; INL, 2016)

Example 18. In 2014 the "Energetic Bear" virus was discovered in over 1,000 energy firms in 84 countries. This virus was used for industrial espionage and because it infected industrial control systems in the facilities, it could have been used to damage those facilities, including wind turbines, strategic gas pipeline pressurization and transfer stations, liquefied natural gas (LNG) port facilities, and electric generation power plants. It has been suggested that state-sponsored attackers wanted to disrupt national scale gas suppliers. (Scheuermann, 2017)

Example 19. On 23 December 2015, hackers compromised information systems of three energy distribution companies in Ukraine (Ivano-Frankivsk Oblast) and temporarily disrupted the electricity supply to consumers. This was a multistage, multisite attack that disconnected seven 110 kV and twenty-three 35 kV substations were switched off, and about 225 000 people were without electricity for a period from 1 to 6 hours. (WEC, 2016)

Example 20. The second attack against the Ukraine was in December 2016 when power cut had amounted to a loss of about one-fifth of Kiev's power consumption. Workstations and SCADA systems, linked to the 330-kilowatt sub-station "North", were compromised. In the latest attack, hackers are thought to have hidden in Ukrenergo's IT network undetected for six months, acquiring privileges to access systems and figure out their workings, before taking methodical steps to take the power offline. (Polityuk et.al, 2017)

Example 21. In August 2017 the Irish electricity transmission system operator EirGrid was a target of a man-in-the-middle attack. The attack first breached Vodafone's Direct Internet Access (DIA) service which was providing Internet access to EirGrid's interconnector site in Wales. Attackers were able to create a Generic Router Encapsulation (GRE) tunnel into the router used by Eirgrid. All traffic through the DIA router were intercepted by the attacker. It was discovered that System Operator for Northern Ireland (SONI) had their data intercepted too. Vodafone and National Cyber Security Centre attribute this attack to state sponsored actor but do not elaborate that estimation further. (Kovanen et.al, 2018)

Example 22. In mid-November 2017, attackers utilized the TRITON sophisticated attack framework to control industrial safety systems at a critical infrastructure facility and accidentally led to a process shutdown. This malware specifically targeted the Triconex Emergency Shut Down (ESD) system. During this sophisticated attack, the attacker utilized many custom intrusion tools to obtain and maintain access to the target's IT and operational technology networks. (SCF, 2020)

3.9 Financial Services Sector

The financial services sector represents a vital component of a nation's critical infrastructure. Financial institutions provide a broad array of products from the largest institutions to the smallest community banks and credit unions. The finance sector is intricately woven into the daily lives of people around the world and is at the very core of global economies. Financial entities allow citizens and organizations worldwide to manage finances, trade, and to operate in different ways. (DHS, 2014; F-Secure, 2019)

Banks are 300% more likely to be attacked than the average industry and were the most attacked target in 2019. Those attacks have increased dramatically since COVID-19. (Fuchs, 2020)

Threat actors have much to benefit from a successful cyber-attack against any financial institution. This threat not only applies to banks, but also to exchanges, asset managers, technology providers, insurers, clearing and settlement houses, as well as supply chains to these institutions. Both state-sponsored and criminal actors have targeted the finance sector to (F-Secure, 2019):

- Steal personal data,
- Monitor the financial activities of specific clients,
- Disrupt or tamper with critical operations,
- Steal money.

The attackers use offensive techniques, which is a more sophisticated type of attacks such as; distractive attacks, targeted ransomware attacks, supply chain attacks, and cryptojacking. Differently motivated cyber attackers using computer viruses, Trojan horses, worms, logic bombs, eavesdropping sniffers, and other tools that can destroy, intercept, degrade the integrity of, or deny access to data. Other potential cyberthreats to the sector include confidentiality and identity breaches. (DHS, 2014; F-Secure, 2019)

Example 23. In 2015 and 2016 a series of cyber-attacks using the SWIFT banking network were reported, resulting in the successful theft of millions of dollars. The attacks were perpetrated by a hacker group known as APT38. If the attribution to North Korea is accurate, it would be the first known incident of a state actor using cyber-attacks to steal funds. The attacks exploited vulnerabilities in the systems of member banks, allowing the attackers to gain control of the banks' legitimate SWIFT credentials. The thieves then used those credentials to send SWIFT funds transfer requests to other banks, which, trusting the messages to be legitimate, then sent the funds to accounts controlled by the attackers. (Corkery, 2016)

Example 24. The Equifax data breach which occurred between May and July of 2017 at the American credit bureau Equifax. Private records of 147.9 million Americans, along with 15.2 million British citizens and about 19,000 Canadian citizens were compromised in the breach, making it one of the largest cybercrimes related to identity theft. The data breach into Equifax was principally through a third-party software exploit that had been patched, but which Equifax had not updated on their servers. Equifax had been using the open-source Apache Struts as its website framework for systems handling credit disputes from consumers. A key security patch for Apache Struts was released on March 7, 2017 after a security exploit was found and all users of the framework were urged to update immediately. Security experts found an unknown hacking group trying to find websites that had failed to update Struts as early as March 10, 2017, as to find a system to exploit. (Fruhlinger, 2020)

Example 25. On September 6, 2020, Banco Estado, the only public bank in Chile and one of the three largest in the country, had to shut down its nationwide operations due to a ransomware cyber-attack launched by REvil. (Carnegie, 2021)

Example 26. On October 23, 2020, a software defect led to a disruption to the European Central Bank’s main payment system for almost 11 hours. (Carnegie, 2021)

3.10 Food and Agriculture Sector

Agriculture is essential for modern society and has been involved in the adoption of information technology to manage production, processing, transportation, distribution and retailing of commodities and food products for decades. The food and agriculture sector is composed of farms, restaurants, and food manufacturing, processing, and storage facilities. It is composed of complex production, processing, and delivery systems and encompasses huge amounts of critical assets. The sector has a highly effective and resilient food supply chain, owing to the size, geographic diversity, and competitive nature of the industry. (DHS, 2014; GOV.UK, 2017; NCC, 2019; Okupa, 2020)

In the heavily mechanized landscape of agriculture, smart technologies and remote administration used in Precision Agriculture (PA) and smart farming creates a new cyber-physical environment. The incorporation of cyber-based technologies and data driven solutions in farm production, food processing, supplier industries, transport of goods, regulatory oversight, marketing sales and communication with consumers creates a paradigm shift. Cloud-based storage of large data sets, use of open-sourced or internet/cloud-based software, and corporate management of proprietary software each increase opportunities for data access by unauthorized users. (Duncan et.al, 2019; Demestichas et.al, 2020)

Agricultural cybersecurity is a rising concern because farming is becoming ever more reliant on computers and Internet access. Like many industries, agriculture is undergoing a digital revolution powered by big data. Computers, robots, sensors, and big data analytics are driving decision making in the search for higher and more sustainable yields. Farms are driving towards a concept of precision agriculture, a data driven methodology for optimizing crop production. Key areas include soil sampling, yield monitors and maps, GPS guidance systems, satellite imaging and automatic section control. (CRI, 2020; Nikander et.al, 2020)

Whether it is wired-up off-road equipment and machinery, high-tech food and grain processing, radio frequency ID-tagged livestock, or global-positioning-system tracking, the agriculture sector depends on information systems to sustain and improve operations, competitiveness, and profitability. Agricultural production and operations will increase dependency on software and hardware applications which are vulnerable to cyber-attacks. (ISA, 2020)

Potential attacks in various smart agricultural systems are mostly related to cybersecurity, data integrity and data loss. Threat scenarios against the food and agriculture sector are (NCC, 2019; Demestichas et.al, 2020; Okupa, 2020, pp. 25-27):

- Leaking of confidential farm data,
- Loss of availability of distribution and storage systems,
- Loss of availability of processing systems,
- Compromised integrity of food assurance systems,
- Farm vehicle collisions with power assets,
- Publishing confidential information that could be damaging from suppliers,
- Rogue data introduction into network,
- Falsification of data to disrupt both crop and livestock,
- The disruption to navigational, positioning and time systems,
- Disruption to communication networks.

In 2018, the U.S. Council of Economic Advisers reported the agricultural sector experienced 11 cyber incidents in 2016. Compared to other sectors the agricultural sector experienced a relatively low number of reported cyber incidents. The total number of incidents were 42 068. (CEA, 2018)

3.11 Governmental Institutions Sector

In the European system of accounts, the general government sector is defined as consisting

> of institutional units which are non-market producers whose output is intended for individual and collective consumption and are financed by compulsory payments made by units belonging to other sectors, and institutional units principally engaged in the redistribution of national income and wealth. (EC, 2020)

The general government sector has subsectors, like central government, state government, local government, and social security funds.

A ministry is a high-level governmental organization headed by a minister and intended to manage a specific sector of public administration. A government or state agency is a permanent or semi-permanent organization in the machinery of government that is responsible for the oversight and administration of specific functions, such as an administration. (Wikipedia)

The main functions of general government units are (EC, 2020):

- To organize or redirect the flows of money, goods and services or other assets among corporations, among households, and between corporations and households; in the purpose of social justice, increased efficiency or other aims legitimized by the citizens,
- To produce goods and services to satisfy households' needs (e.g., state health care) or to collectively meet the needs of the whole community (e.g., defense, public order and safety).

Many government agencies are tasked with providing new technology and services to citizens as quickly and efficiently as possible for a plethora of functions. Government entities frequently have access to a lot of personally identifiable information and other types of data that would be disastrous if an attacker got their hands on it.

Cyber-attacks against state and local governments have been dramatically increasing. In 2019 in the U.S. alone, there were 140 ransomware attacks – an average of 3 per day – targeting public, state, and local government and healthcare providers in the US. This is up 65% from the previous year. (Orr, 2020)

A key factor contributing to the rise of attacks on local government agencies is the commoditization of attack techniques. Ransomware is not new, but the hacker community is able to deploy the attacks quickly, easily, and highly successfully. Hackers are using more sophisticated attack methods and are sharing their knowledge readily with others. Ransomware is also growing in popularity because attackers know government agencies are highly likely to pay since their cyber-attack recovery readiness is often low, and because the alternative – denial of government services – is unacceptable. (Kennedy, 2019)

Synack's trust report (Synack, 2020) tells that the government sector is globally the most hardened against cyber-attacks in 2020. It was discovered that governments scored 15% higher respectively than all other industries when it came to preventing attacks and responding to breaches. Government agencies earned the top spot in part due to reducing the time it takes to remediate exploitable vulnerabilities by 73%.

Example 27. Two separate attacks were launched on the U.S. Office of Personnel Management between 2012 and 2015. Hackers stole around 22 million records. The information that was obtained and exfiltrated in the breach included personally identifiable information such as social security numbers, as well as names, dates and places of birth, and addresses. Chinese state-sponsored hackers were accused of the attack. (Wikipedia)

Example 28. The 2013 data hack at the Finnish Foreign Ministry was perpetrated by a group of Russian hackers and was part of a wider campaign against targets in nearly fifty countries. Experts have identified that the attack was perpetrated by the Turla group. It is widely believed that the Turla group is the premier Russian hacker organization and it targets ministries, embassies, and militaries in Russia's neighbors. Kaspersky has seen traces in malware and servers, that point to the fact that the authors are Russian speaking, and they seem to have a lot of resources for their cyber espionage operation. (Yle, 2016)

Example 29. The Finnish Parliament was the target of a cyber-attack during the autumn of 2020. As a result of the attack, the security of several parliamentary email accounts was compromised, some of which belonged to MPs. The attack was detected by Parliament's internal technical surveillance. (Yle, 2020)

Example 30. In September 2020 the Norwegian parliament announced it had been the target of a significant cyber-attack which breached the email accounts of several members and staff of Norway's Labor Party. (OAGOV, 2020)

Example 31. In the fall of 2020, a major cyber-attack by a group backed by a foreign government, penetrated multiple parts of the US Federal Government, leading to a series of data breaches. The hacking group Cozy Bear (APT29) was identified as the cyber attackers. The cyber-attack and data breach were reported to be among the worst cyber-espionage incidents ever suffered by the U.S., due to the sensitivity and high profile of the targets and the long duration (eight to nine months) in which the hackers had access. The attackers exploited software from at least three U.S. firms: Microsoft, SolarWinds, and VMware. (Geller, 2020)

3.12 Healthcare Sector

The healthcare sector is responsible for protecting and sustaining the citizen's health. Health services are divided into primary health care and specialized medical care. This widespread and diverse sector includes acute care hospitals, ambulatory healthcare, national, and local public health systems; disease surveillance; and private sector industries that manufacture, distribute, and sell drugs, biologics, and medical devices. (DHS, 2014)

Cyber-attacks against the healthcare sector are especially concerning because these attacks can directly threaten not just the security of systems and information but also the health and safety of patients. Hospitals are especially sensitive to cyber-attacks as any disruption in operations or even disclosure of patient personal information can have far-reaching consequences.

The healthcare sector is one of the most frequently breached industries in the world. This sector has an abundance of sensitive data and Personal Identifiable Information (PII) that can be exploited by hackers within healthcare organizations. According to a CBS report, medical records can sell for up to $1,000 each on the dark web, while social security numbers and credit cards sell for $1 and up to $110, respectively (Wandera, 2020). Data breaches cost the health care industry approximately $5.6 billion every year.

High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks (Swivel, 2020):

- Private patient information is worth a lot of money to attackers,
- Medical devices are an easy entry point for attackers,
- Staff need to access data remotely, opening-up more opportunities for attack,
- Workers do not want to disrupt convenient working practices with the introduction of new technology,
- Healthcare staff are not educated in online risks,
- The number of devices used in hospitals makes it hard to stay on top of security,
- Healthcare information needs to be open and shareable,
- In smaller healthcare organizations, cybersecurity is often poorly managed,
- Outdated technology means the healthcare industry is unprepared for attacks.

The threat vectors against healthcare systems are: E-mail phishing attacks, ransomware attacks, man-in-the-middle attacks, loss or theft of medical equipment or data (PII), insider, accidental or intentional data loss, attacks against connected medical devices.

Based on Wandera's (2020) research, the highest risks and the percentage of healthcare organizations affected by each one is:

- Malicious network traffic: 72 %,
- Phishing: 56 %,
- Vulnerable OS (old version): 48 %,
- Man-in-the-middle attack: 16 %,

- Malware: 8 %.

The US Department of Health and Human Services' (HHS) breach portal contains information about breaches of Protected Health Information (PHI). According to the HHS breach portal, data breaches affected 27 million people in 2019 in U.S. Top 10 breaches by number of individuals affected, currently listed on HHS's breach portal, are given in Table 1. (HHS, 2020)

Table 1. Top 10 breaches by number of individuals affected in US

Name of covered entity	Covered entity type	Individuals affected	Type of breach	Location of breached information	Year
Anthem Inc.	Health Plan	78 800 000	Hacking/IT Incident	Network Server	2015
American Medical Collection Agency	Business Associate	26 059 725	Hacking/IT Incident	Network Server	2019
Optum360, LLC	Business Associate	11 500 000	Hacking/IT Incident	Network Server	2019
Premera Blue Cross	Health Plan	11 000 000	Hacking/IT Incident	Network Server	2015
Laboratory Corporation of America	Health Plan	10 251 784	Hacking/IT Incident	Network Server	2019
Excellus Health Plan, Inc.	Health Plan	10 000 000	Hacking/IT Incident	Network Server	2015
Community Health Systems Professional Services Corporations	Healthcare Provider	6 121 158	Hacking/IT Incident	Network Server	2014
Science Applications International Corporation	Business Associate	4 900 000	Loss	Other	2011
Community Health Systems Professional Services Corporation	Business Associate	4 500 000	Theft	Network Server	2014
University of California, Los Angeles Health	Healthcare Provider	4 500 000	Hacking/IT Incident	Network Server	2015

Medical devices include all those devices (hardware and software) used in patient care for diagnosis, treatment, and monitoring. This extends to ancillary support devices that are required for the medical device to function properly and are hosted on a clinical network such as external disk storage, database servers, and gateway or middleware interface devices. Security incidents related to medical devices also have the potential to impact patient safety and do meaningful harm to patients connected to these networked devices. (Department of Health, 2018)

Medical devices have become a cyber-attack target for many reasons. Medical devices are increasingly network connected, using default passwords, missing patches, remote access, and other weaknesses. So, the main vulnerabilities are application vulnerabilities, unpatched software, and configuration vulnerabilities. (Department of Health, 2018)

Example 32. In May 2017 WannaCry malware spread like a worm laterally in the network which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It propagated through EternalBlue exploit. One infected organization was the National Health Service's (created in 1948) hospitals in England and Scotland. Up to 70,000 devices including computers, MRI scanners, blood-storage refrigerators and theatre equipment have been affected. Ambulances diverted and disruption to surgeries. No patient data was affected and there was no access to prescriptions or medical histories for treatment. 200,000 machines in 150 countries were affected. (Wikipedia)

Example 33. A ransomware attack struck a hospital in Düsseldorf on September 10, 2020. The cyber-attack caused network outages that forced the clinic to reroute patients in need of emergency care elsewhere. One 78-year-old woman who required immediate attention for an aneurysm died after being sent to another city. The case is still under investigation. (Hackett, 2020)

Example 34. In autumn of 2020 the healthcare industry detected cyber-attacks from three nation-state actors targeting seven prominent companies directly involved in researching vaccines and treatments for Covid-19. The targets include leading pharmaceutical companies and vaccine researchers in Canada, France, India, South Korea, and the United States. The attacks came from Strontium, an actor originating from Russia, and two actors originating from North Korea that are called Zinc and Cerium. (Burt, 2020)

3.13 Information Technology Sector

The information technology sector is central to the nation's security, economy, and public health and safety as businesses, governments, academia, and private citizens are increasingly dependent upon information technology sector functions. These virtual and distributed functions produce and provide hardware, software, and information technology systems and services, and the Internet. (DHS, 2014)

The IT sector is highly concerned about cyber threats, particularly those that degrade the confidentiality, integrity, or availability of the sector's critical functions. Depending on its scale, a cyber-attack could be debilitating to the IT sector's highly interdependent critical infrastructures. The cyber threats include unintentional acts (e.g., the accidental disruption of Internet content services) and intentional acts (e.g., the exploitation of IT supply chain vulnerabilities or the loss of interoperability between systems as the result of an attack). (DHS, 2014)

Cyber-attacks are increasingly targeting the technology sector. Technology became the most attacked industry for the first time, accounting for 25% of all attacks (up from 17%). Over half of attacks aimed at this sector were application-specific (31%) and DoS/DDoS (25%) attacks, as well as an increase in weaponization of IoT attacks. (Williams, 2020)

Organizations in the high tech and information technology industry face cyber threats from the following actors (FireEye, 2016):

- Advanced persistent threat (APT) groups seeking to steal economic and technical information to support the development of domestic companies through reducing research and development costs, or otherwise providing a competitive edge.
- Hacktivists and cyber vandals with disruptive motivations may target Internet service providers to gain attention for their cause.

Some parts of the IT and high-tech sector provide an attack path into other sectors since IT products are a key infrastructure component for all kinds of organizations. Cloud storage providers, cloud computing services, developers of cyber security software, or a file-sharing solution provider, are often the targets of cyber-attacks. Partnerships with government or military entities would likely also place companies at risk, as foreign state-sponsored threat actors would probably target such companies. (FireEye, 2016; Papesh, 2019)

The development of new technologies will likely spur threat activity against the industry. One of the biggest threats for the high-tech sector companies is the loss of intellectual property. Having intellectual property lost or stolen after years of investment can dramatically reduce an organization's competitive advantage. High-tech companies create products that some technically skilled people want to use maliciously. IT tools can be used to implement hacking and cyber intelligence. (Deloitte, 2021)

3.14 Nuclear Sector

The nuclear sector covers most aspects of civilian nuclear infrastructure: from the power reactors that provide electricity to citizens, to the medical isotopes used to treat cancer patients. The nuclear sector includes nuclear power plants, research and test reactors, fuel cycle facilities, radioactive waste management, decommissioning reactors, nuclear and radioactive materials used in medical, industrial, and academic settings, and nuclear material transport. (DHS, 2014)

The vulnerability of nuclear plants to create a deliberate attack is of concern in nuclear safety and security. Cyber-attacks on the nuclear sector infrastructure and assets by terrorists, extremists, or foreign actors can target the industrial control systems or SCADA. Attacks may pose a significant threat to the sector, allowing malicious actors to manipulate or exploit facility operations. Cyber-attacks on nuclear power plants could have physical effects, especially if the network that runs the machines and software controlling the nuclear reactor are compromised. This can be used to facilitate sabotage, theft of nuclear materials, or in the worst-case scenario a reactor meltdown. (DHS, 2014; Das, 2019)

Example 35. The Stuxnet worm affected Iran's nuclear development capabilities in 2010. Stuxnet specifically targets Programmable Logic Controllers (PLCs), which allow the automation of electromechanical processes such as those used to control machinery and industrial processes including gas centrifuges for separating nuclear material. Stuxnet caused a malfunction that was invisible to human operators because the SCADA screens in the control room suggested normal operation. (Falliere et.al, 2011)

Example 36. The South Korean nuclear and hydroelectric company Korea Hydro and Nuclear Power (KHNP) was hacked in December of 2014. Hackers stole and posted online the plans and manuals for two nuclear reactors, as well as the data of 10,000 employees. South Korean authorities traced the IP addresses to Shenyang, a city in north-east China. (Macola, 2020)

Example 37. In April 2016 Gundremmingen nuclear power facility had been harboring malware, including remote-access trojans and file-stealing malware, on the computer system that is used to monitor the plant's fuel rods. Fortunately, the computer was not connected to the Internet, and the malware was never able to be activated. (Gallagher, 2016)

Example 38. The Nuclear Power Corporation of India Limited (NPCIL) reported that there was a cyber-attack on the Kudankulam Nuclear Power Plant (KKNPP) in September of 2019. The nuclear power plant’s administrative network was breached in the attack but did not cause any critical damage. (Das, 2019)

3.15 Transportation Systems Sector

The transportation systems sector is comprised of the road, aviation, rail, and maritime sub-sectors. Most of the transport operates on a commercial basis, with responsibility for resilience delegated to owners and operators. The transportation systems sector moves people and goods through the country and overseas. Transport networks are essential for maintaining the health, safety, security, and social and economic well-being of citizens. DHS, 2014; ENISA, 2015; GOV.UK, 2017)

The aviation sector is a cornerstone of national and international commerce, trade, and tourism, which means even an isolated incident could spark a crisis of confidence in the entire sector. The aviation sector consists of airports, air traffic control facilities, and air navigation facilities. (ENISA, 2015; Lehto, 2020)

The maritime sector is a vital part of the global economy, whether it is carrying cargo, passengers, or vehicles. Ships are becoming increasingly complex and dependent on the extensive use of digital and communications technologies throughout their operational life cycle. The maritime transportation system is a geographically and physically complex and diverse system consisting of waterways, ports, and intermodal landside connections. (DHS, 2014; Lehto, 2020)

The cyber security risk landscape in transport is currently evolving towards the point that risks that were once considered unlikely began occurring with regularity. Disruption to the transport network has significant impacts on the everyday life of citizens, national defense, security, and the vital functions of the state. One challenge in the transportation sector is that some legacy transportation systems now interface with public applications for ticketing and scheduling and rely on networked devices for routing, positioning, tracking and navigation. This presents multiple potential entry points for hackers. (DHS, 2014; Lehto, 2020; Knott, 2020)

The threat vectors against transportation systems are among others (ENISA, 2015):

- Distributed Denial of Service attacks (DDoS),
- Manipulation of hardware and/or software,
- Malware and viruses,
- Tempering and/or alteration of data including insertion of information,
- Hacking of wireless, connected assets,
- Identity theft,
- Exploitation of software bugs,
- Abuse of authorization,
- Abuse of information leakages,
- E-mail phishing attacks,
- Ransomware attacks,
- Man-in-the-middle attacks,
- Insider, accidental or intentional data loss (data breaches).

Cybersecurity is a growing concern for civil aviation, as organizations increasingly rely on electronic systems for critical parts of their operations, including safety-critical functions. From ransomware attacks to data breaches, the transportation sector is not immune to malicious hackers. A concerted, well-orchestrated attack on any aviation sub system and network could cause a considerable disruption sector-wide. (DHS, 2014; Lehto, 2020)

The maritime transport industry is highly exposed to cyber-attacks. Vessels do not need to be attacked directly. An attack can arrive via a company's shore-based information technology systems and very easily penetrate a ship's critical onboard operational technology systems. These systems are used for a variety of purposes, including access control, navigation, traffic monitoring, and information transmission. Although the interconnectivity and utilization of the cyber systems facilitate transport, they can also present opportunities for exploitation, contributing to risk for the maritime systems. (DHS, 2014; Lehto, 2020)

There are several reasons for conducting cyber-attacks against the transportation sector. Due to the reliance of trade on the sector, an attack could be used to affect trade in general, or even target a specific commodity and its availability. Due to the interdependence of the various transport infrastructures, there are a variety of targets to impact the trade: Railways or roads could be targeted to prevent goods reaching the ports and disrupting the ports themselves would hinder any import or export.

Airports can be targeted to affect tourism, material transportation or business travel. Similarly, disrupting operations could delay military deployments or operations. Cyber-attacks could potentially be seen as the modern version of a Naval blockade. The greatest fear faced by transportation agencies is the potential for accidents, mass chaos, and even injuries or loss of life due to disruptions to critical infrastructure. (van Niekerk, 2018)

Example 39. In 2015 an attack on the IT network of the LOT airline of Poland caused at least 10 flights to be grounded. It was one of the first reported cases of hackers causing cancellations. LOT encountered an IT attack that affected the ground operation systems. As a result, LOT was not able to create flight plans and outbound flights from Warsaw are not able to depart. The attack caused journeys from Warsaw to a range of European destinations to be terminated, including trips to Munich, Hamburg, Copenhagen, and Stockholm, amongst others. As many as 1500 passengers were said to have been affected. (Brewster, 2015)

Example 40. Cyber breach affecting Cosco's operations in the US Port of Long Beach, on 24 July 2018, which affected the giant’s daily operations. The company’s network broke down, and some electronic communications were not available as a result. (Safety4Sea, 2018)

Example 41. Petya malware variant infected the IT systems of the world’s largest shipping company Maersk with 600 container vessels handling 15% of the world’s seaborne trade in June 2017. The breakdown affected all business units at Maersk, including container shipping, port and tugboat operations, oil, and gas production, drilling services, and oil tankers. Maersk reporting up to $300 million in losses. (Gronholt-Pedersen, 2017)

Example 42. In 2016, the light rail system in San Francisco was hacked, halting access to agency emails and the computer system while hackers demanded 100 bitcoin payment to unlock the hacked computer systems, which the department refused to pay. But rather than shut down the network, the attack simply led to machines being turned off and passengers were allowed to grab free rides. (Brewster, 2016)

Example 43. A team of experts in the US Homeland Security team remotely hacked a Boeing 757. This hack was not conducted in a laboratory, but on a 757 parked at the airport in Atlantic City. The team got the airplane on September 19, 2016 and two days later, an expert was successful in accomplishing a remote, non-cooperative, penetration. (CSO, 2017)

3.16 Water and Wastewater Systems Sector

The water and wastewater systems sector offers drinking water to citizens which is a prerequisite for protecting public health and all human activity. Properly treated wastewater is vital for preventing disease and protecting the environment. The sector is comprised of public drinking water systems (includes both community and non-community water systems, such as schools, factories, and other commercial or governmental facilities) and wastewater treatment utilities. Water utilities consist of water sources, treatment facilities, pumping stations, storage sites, and extensive distribution, collection, and monitoring systems. (DHS, 2014)

Water utilities around the world are vulnerable to attacks because they are usually small and have almost no cybersecurity expertise among staff members (Brumfield, 2020). Cyber-attacks on water and wastewater systems sector infrastructure and assets by terrorists, extremists, or foreign actors can target the industrial control systems or SCADA. The cyber-attacks targeting the water sector are complex and sophisticated, and they are often orchestrated by state-sponsored bodies whose objective is to destabilize a country's economy (Ben Boubaker, 2020).

Our dependency on water – e.g., for consumption, hygiene, agriculture, industry, or energy production – provides an inviting environment for cyber attackers. The effects of a cybersecurity attack on the critical water sector operations could cause devastating harm to public health and safety, threaten national security and result in costly recovery and remediation efforts to address system issues as well as data loss. (DHS, 2014; Germano, 2019).

Example 44. A water department in the state of North Carolina was targeted by a cyber-attack using ransomware in 2018. It began on October 4th when the system was hit with Emotet, an advanced, modular banking Trojan that primarily functions as a downloader or dropper of another banking Trojan. IT staff members were unsuccessful in stopping the ransomware infection from spreading, so the crypto virus spread quickly along the network, encrypting databases and files. The water utility did not pay the ransoms (CSO, 2018)

Example 45. Two cyber-attacks hit Israel's water system in 2020. The first attack hit in April when hackers tried to modify the waters chlorine levels. The first attack hit agricultural water pumps in upper Galilee, while the second one hit water pumps in the central province of Mateh Yehuda. The attempted attacks were unsuccessful. (Cimpanu, 2020)

4 Critical Infrastructure Protection

Industrial control system cyber-attacks require a lot of knowledge and planning. ICS attacks take a long time to launch because adversaries must know a lot about the systems. Industrial control systems are not just digital; they are also analog and mechanical. Usually, critical infrastructure system has all different kinds of combinations of those things in industrial environment as well as having digital PLCs that are programmed to do things, as well as DCS and SCADA systems. (Brumfield, 2020)

Building a cybersecurity critical infrastructure program takes time, careful planning, and ongoing support from political leadership, state level agencies, and public and private entities overseeing critical infrastructure. The first step is helping key players in government understand the severity, urgency, and potential impacts of different types of cyber threats and the need to take immediate action. (Deloitte, 2017)

The implementation of protective measures aimed at securing critical infrastructure systems requires a considered and holistic approach, as there are many variables involved in establishing and maintaining a balance between security and functionality of service delivery and system availability. A key part of the greater national infrastructure security situational picture is the continued availability of critical infrastructure systems. (Warren et al., 2010)

In the EU's view, strong cyber resilience needs a collective and wide-ranging approach. This calls for more robust and effective structures to promote cybersecurity and to respond to cyber-attacks in the Member States but also in the EU's own institutions, agencies, and bodies. It also requires a more comprehensive, cross-policy approach to building cyber-resilience and strategic autonomy, with a strong Single Market, major Advances in the EU's technological Capability, and far greater numbers of skilled experts. At the heart of this is a broader acceptance that cybersecurity is a common societal challenge, so that multiple layers of government, economy and society should be involved. (EC, 2017)

Managing the risks from significant threat and hazards to physical and cyber critical infrastructure requires an integrated and comprehensive approach across this diverse community. The U.S. National Infrastructure Protection Plan (NIPP) defines the objectives as identify, deter, detect, disrupt, and prepare for threats and hazards to the nation's critical infrastructure, reduce vulnerabilities of critical assets, systems, and networks, mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur. (DHS, 2013)

There are controls that every critical infrastructure organization should consider. These controls are categorized as (Hassanzadeh et al., 2020):

- Basic Controls, such as inventory and control of hardware/software assets, continuous vulnerability management, or controlled use of administrative privileges,
- Foundational Controls, such as email and web browser protections, malware defenses, or secure configuration for network devices like firewalls, routers, and switches,
- Organizational Controls, such as the implementation of a security awareness and training program, incident response and management, penetration tests, and red team exercises.

The U.S. President’s National Infrastructure Advisory Council (NIAC) (NIAC, 2017) suggests following decisive cyber security actions:

1. Establish separate, secure communications networks specifically designated for the most critical cyber networks, including “dark fiber” networks for critical

control system traffic and reserved spectrum for backup communications during emergencies.

2. Identify best-in-class scanning tools and assessment practices, and work with owners and operators of the most critical networks to scan and sanitize their systems on a voluntary basis.
3. Strengthen the capabilities of today's cyber workforce by sponsoring a public-private expert exchange program.
4. Establish a set of limited time, outcome-based market incentives that encourage owners and operators to upgrade cyber infrastructure, invest in state-of-the-art technologies, and meet industry standards or best practices.
5. Establish clear protocols to rapidly declassify cyber threat information and proactively share it with owners and operators of critical infrastructure, whose actions may provide the nation's front line of defense against major cyber-attacks.

5 Conclusion

The continuous and rapid digitization at a global level, underpinned by the progress made in smart ICT as well as the integration of IoT and automation, is a trend that deeply transforms many market sectors and has created opportunities in several areas of global economies and societies. So, smart ICT and IoT is the backbone of the fourth industrial revolution and are basic elements of the critical infrastructure. (Demestichas et al., 2020)

The issue of cyber security in the fourth industrial revolution is currently having and will continue to have a significant impact on the critical infrastructure. As Industrial Control Systems, SCADA, Distributed Control System, Operational Technology, and other process control networks are Internet-connected, they expose crucial services to cyber-attacks. Extremely sophisticated cyber-attacks such as the Duqu and the Stuxnet worm show how effectively critical infrastructure can be attacked.

Cyber-attacks directed against critical infrastructure organizations can be conducted in many forms, which may consist of a single act or a combination of discrete steps threaded together. Such acts may be a Complicated exploitation of coding or the simple use of social engineering to reveal or to gain access to confidential information. Once the targeted system is compromised, perpetrators might implement "back door" Gates or install Stealth code allowing information to be monitored or removed without detection. "Kill switches" can be implemented, which can be activated at a specified time or under a specified set of conditions. System control allows an attacker to paralyze or even destroy a system. (APTA, 2014)

The structure and operation of modern highly networked critical infrastructure systems fundamentally depends on networked information systems, some of which have unfortunately been inadequately secured from cyber-attacks. The vulnerabilities also make CI systems highly vulnerable to hybrid warfare tactics of both state and non-state actors. The combined complexities of these networked systems interacting together stands to amplify threats and vulnerabilities that exist in any of the major systems, as well as risk to other dependent systems.

Major attacks on critical infrastructure such as power, gas, and water stations, as well as transportation control systems, have become the new face of warfare. In October 2019, hackers knocked out more than 2,000 websites hosted in the nation of Georgia. According to the U.K., the U.S., and Georgia, Russia carried out this attack to destabilize the country as part of its hybrid warfare activities. (Breth and Douglas, 2020)

It will be increasingly difficult to distinguish cyber sabotage operations from hybrid warfare operations. Developments could lead to serious crises around the world. Many security officials have been warned of a "cyber tsunami or 9/11," which could trigger a cyberwar that will unleash reactions that cannot be controlled.

References

Abomhara M. and. Køien G.M. (2015). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 4(1): 65-88. Doi: 10.13052/jcsm2245-1439.414.

AP (2015). Iranian hackers infiltrated U.S. power grid, dam computers, reports say. Posted by the Associated Press, CBC/Radio-Canada, https://www.cbc.ca/news/technology/hackers-infrastructure-1.3376342

APTA (2014). Cybersecurity considerations for public transit. Report APTA SS-ECS-RP-001-14, American Public Transportation Association, Washington, DC. https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-ECS-RP-001-14-RP.pdf

Ashenden D. (2011). Cyber security: Time for engagement and debate. In European Conference on Information Warfare and Security, pp. 11-16. Academic Conferences.

Ballou T., Allen J.A., Francis K.K. (2016). U.S. energy sector cybersecurity: Hands-off approach or effective partnership? *Journal of Information Warfare*, 15(1):44-59.

Beggs C. (2006). Proposed risk minimization measures for cyber-terrorism and SCADA networks in Australia. In *ECIW 2006 – 5th European Conference on Information Warfare and Security*. Academic Conferences.

Ben Boubaker K. (2020). Water infrastructure: When states and cyber-attacks rear their ugly heads. Stormshield, https://www.stormshield.com/news/water-infrastructure-when-states-and-cyber-attacks-rear-their-ugly-heads/

Bertino E., Martino L.D., Paci F., and Squicciarini A.C. (2010). Web services threats, vulnerabilities, and countermeasures. In Security for Web Services and Service-Oriented Architectures, pp. 25–44. Springer.

Biancuzzo M.R. (2017). Cybersecurity & critical infrastructure. Briefing Papers, issue 17-13, Thomson Reuters.

Brenner B. (2011). Nitro attack: Points of interest. CSO, https://www.csoonline.com/article/2134921/nitro-attack--points-of-interest.html

Breth J. and Douglas C. (2020). Cybersecurity needs its place in emergency management now. CPO Magazine, https://www.cpomagazine.com/cyber-security/cybersecurity-needs-its-place-in-emergency-management-now/

Brewster T. (2015). Attack on LOT Polish airline grounds 10 flights. Forbes, https://www.forbes.com/sites/thomasbrewster/2015/06/22/lot-airline-hacked/?sh=3862c062124e

Brewster T. (2016). Ransomware Crooks demand $70,000 after hacking San Francisco transport system. Forbes, https://www.forbes.com/sites/thomasbrewster/2016/11/28/san-francisco-muni-hacked-ransomware/?sh=ae56b3847061

Brumfield C. (2020). Attempted cyberattack highlights vulnerability of global water infrastructure. CSO, https://www.csoonline.com/article/3541837/attempted-cyberattack-highlights-vulnerability-of-global-water-infrastructure.html

Burt T. (2020). Cyberattacks targeting health care must stop. Microsoft. https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/

Carnegie (2021). Timeline of cyber incidents involving financial institutions. Carnegie, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline, retrieved 24 January 2021.

CEA (2018). The cost of malicious cyber activity to the U.S. economy. Council of Economic Advisers, White House, Washington, DC.

Chong J. (2013). Why is our cybersecurity so insecure? New Republic, https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure

Cimpanu C. (2020). Two more cyber-attacks hit Israel's water system. ZDNet, https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/

CISA (2019). Chemical sector landscape. Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security.

Constantin L. (2021). 33 hardware and firmware vulnerabilities: A guide to the threats. CSO, https://www.csoonline.com/article/3410046/hardware-and-firmware-vulnerabilities-a-guide-to-the-threats.html

Corkery, M. (2016). Once again, thieves enter swift financial network and steal. New York Times, https://www.nytimes.com/2016/05/13/business/dealbook/swift-global-bank-network-attack.html

CRI (2020). Cyber threats to the agriculture sector. Cyber Risk International, https://cyberriskinternational.com/2020/04/07/cyber-threats-to-the-agriculture-sector/

CrowdStrike (2020). 2020 global threat report. CrowdStrike.

CSO (2017). Homeland Security team remotely hacked a Boeing 757. CSO, https://www.csoonline.com/article/3236721/homeland-security-team-remotely-hacked-a-boeing-757.html

CSO (2018). Ransomware attack hits North Carolina water utility following hurricane. CSO, https://www.csoonline.com/article/3314557/ransomware-attack-hits-north-carolina-water-utility-following-hurricane.html

Das D. (2019). An Indian nuclear power plant suffered a cyberattack: Here's what you need to know. The Washington Post, https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/

Department of Health (2018). Medical device cyber security - Draft guidance and information for consultation, Australia's Therapeutic Goods Administration (TGA), 19.12.2018

Deloitte (2017). Cybersecurity for critical infrastructure: Growing, high-visibility risks call for strong state leadership. Deloitte, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-public-sector-cybersecurity-critical-infrastructure.pdf

Deloitte (2021). Global cyber executive briefing: High technology. Case studies, Deloitte Development LLC. https://www2.deloitte.com/ba/en/pages/risk/articles/High-Technology-Sector.html, retrieved 13 January 2021.

Demestichas K., Peppes N., and Alexakis T. (2020). Survey on security threats in agricultural IoT and smart farming. *Sensors*, 20(22):6458. Doi: 10.3390/s20226458

DHS (2010a). Defense Industrial Base Sector-Specific Plan: An annex to the National Infrastructure Protection Plan. U.S. Department of Homeland Security.

DHS (2010b). Emergency Services Sector-Specific Plan: An annex to the National Infrastructure Protection Plan. U.S. Department of Homeland Security.

DHS (2012). Emergency Services Sector Cyber Risk Assessment. U.S. Department of Homeland Security.

DHS (2013). NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. U.S. Department of Homeland Security.

DHS (2014). Sector risk snapshots. U.S. Department of Homeland Security.

DHS (2015). Dams Sector-Specific Plan: An annex to the NIPP 2013. U.S. Department of Homeland Security.

DHS (2015b). Commercial Facilities Sector-Specific Plan: An annex to the NIPP 2013. U.S. Department of Homeland Security.

DHS (2016). Introduction to the Commercial Facilities Sector-Specific Agency. https://zahp.org/wp-content/uploads/2018/01/commercial-facilities-ssa-fact-sheet-2016-508.pdf

DHS (2020). Critical infrastructure security. U.S. Department of Homeland Security, https://www.dhs.gov/topic/critical-infrastructure-security

Duncan S.E., Reinhard R., Williams R.C., Ramsey F., Thomason W., Lee K., Dudek N., Mostaghimi S., Colbert E., and Murch R. (2019). Cyberbiosecurity: A new perspective on protecting U.S. food and agricultural system. *Frontiers in Bioengineering and Biotechnology*, 7: 63.

Dunn Cavelty, M. (2010). The reality and future of cyberwar. Parliamentary Brief, www.parliamentarybrief.com/2010/03/the-reality-and-future-of-cyberwar Can't reach this page!

EC (2005). On a European programme for critical infrastructure protection. Green paper, COM(2005) 0576 final, European Commission.

EC (2006). On a European programme for critical infrastructure protection. Communication from the Commission, COM(2006) 786 final, European Commission.

EC (2007). Towards a general policy on the fight against cyber crime. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, COM(2007) 267 final, European Commission.

EC (2017). Resilience, deterrence and defence: Building strong cybersecurity for the EU. Joint communication to the European Parliament and the Council, JOINT(2017) 450 final, European Commission.

EC (2020). Glossary: General government sector. European Commission, https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:General_government_sector, retrieved 25 January 2021.

EECSP (2017). Cyber security in the energy sector: Recommendations for the European Commission on a European strategic framework and potential future legislative acts for the energy sector. EECSP Report, Energy Expert Cyber Security Platform.

ENISA (2015). Cyber security and resilience of intelligent public transport: Good practices and recommendations. European Union Agency for Network and Information Security (ENISA).

EU (2008). On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Council Directive 2008/114/EC. *Official Journal of the European Union*, L 345:75-82.

Falliere N., Murchu L.O, and Chien E. (2011). W32.Stuxnet dossier, version 1.4. Wired, https://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf

FCC (2014). Cyber security planning guide. Federal Communications Commission (FCC).

Finkle J. (2011). Government facilities targets of cyber attacks. Reuters, https://www.reuters.com/article/us-usa-hackers-idUSTRE7656M020110706

FireEye (2016). Cyber threats to the high tech and IT industry. FireEye, Milpitas, CA, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-high-tech.pdf

Fruhlinger J. (2020). Equifax data breach FAQ: What happened, who was affected, what was the impact? CSO, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

F-Secure (2019). Cyber threat landscape for the finance sector. F-Secure.

Fuchs J. (2020). Why the biggest threat to financial firms is cyber attacks. Avanan, https://www.avanan.com/blog/biggest-threat-financial-firms-cyber-attacks

Gallagher S. (2016). German nuclear plant's fuel rod system swarming with old malware. Ars Technica, https://arstechnica.com/information-technology/2016/04/german-nuclear-plants-fuel-rod-system-swarming-with-old-malware/

Geller E. (2020). 'Massively disruptive' cyber crisis engulfs multiple agencies. Politico, https://www.politico.com/news/2020/12/14/massively-disruptive-cyber-crisis-engulfs-multiple-agencies-445376

Germano J.H. (2019). Cybersecurity risk & responsibility in the water sector. American Water Works Association.

Gonzales D., Harting S., Adgie M.K., Brackup J., Polley L., and Stanley K.D. (2020). Unclassified and secure: A defense industrial base cyber protection program for unclassified defense networks. RAND Corporation, Santa Monica, CA.

Goodin D. (2018). Hackers infect 500,000 consumer routers all over the world with malware. Ars Technica, https://arstechnica.com/information-technology/2018/05/hackers-infect-500000-consumer-routers-all-over-the-world-with-malware/

GOV.UK (2017). Public Summary of Sector Security and Resilience Plans. Cabinet Office, London.

GOV.UK (2019). Common cyber attacks: Reducing the impact. National Cyber Security Centre.

Gronholt-Pedersen J. (2017). Maersk says global IT breakdown caused by cyber attack. Reuters, https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO

GSMA (2019). Mobile telecommunications security threat landscape. GSM Association, London.

Hackett R. (2020). Ransomware attack on a hospital may be first ever to cause a death. Fortune, https://fortune.com/2020/09/18/ransomware-police-investigating-hospital-cyber-attack-death/

Hassanzadeh A., Rasekh A., Galelli S., Aghashahi M., Taormina R., Ostfeld A., and Banks M.K. (2020). A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, 146(5): 03120003.

Hess E. (2019). People, process, and technology: The trifecta of cybersecurity programs. Helical, https://helical-inc.com/blog/people-process-and-technology-the-trifecta-of-cybersecurity-program/

HHS (2020). Breach portal: Notice to the secretary of HHS breach of unsecured protected health information. U.S. Department of Health & Human Services, Washington, DC, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, retrieved 13 January 2021.

Hollis D. (2011). Cyberwar case study: Georgia 2008. Small Wars Journal, https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008

HVK (2020). Kriittinen infrastruktuuri. Huoltovarmuuskeskus, https://www.huoltovarmuuskeskus.fi/sanasto#k

INL (2016). Cyber threat and vulnerability analysis of the U.S. electric sector. Mission Support Center Analysis Report, Idaho National Laboratory.

ISA (2020). Cybersecurity in the food and agriculture sector. Internet Security Alliance, Arlington, VA, https://isalliance.org/sectors/agriculture/

Jones S.R. (2017). The impact that a cyber-attack would cause within the emergency services sector. Master's thesis, Utica College, ProQuest LLC, Ann Arbor, MI.

Kaspersky (2016). Threat intelligence report for the telecommunications industry. Kaspersky Lab.

Kennedy C. (2019). Government networks are under cyber attack: Here's how cities, agencies can fight back. Homeland Security Today, https://www.hstoday.us/subject-matter-areas/infrastructure-security/government-networks-are-under-cyber-attack-heres-how-cities-agencies-can-fight-back/

Knott F. (2020). The threat of cybercrime for state and local transportation systems. Attila Security, https://www.attilasec.com/blog/transportation-systems-cybercrime, retrieved 13 January 2021.

Kovacs E. (2020). Telecom sector increasingly targeted by Chinese hackers: CrowdStrike. Security Week, https://www.securityweek.com/telecom-sector-increasingly-targeted-chinese-hackers-crowdstrike

Kovanen T., Nuojua V., and Lehto M. (2018). Cyber threat landscape in energy sector. In *ICCWS 2018: Proceedings of the 13th International Conference on Cyber Warfare and Security*, pp. 353-361. Academic Conferences International.

Kumar V. (2020). Cybersecurity challenges and solutions in the telecom industry. Industry Wired, https://industrywired.com/cybersecurity-challenges-and-solutions-in-the-telecom-industry/

Kuokkanen N. (2020). Kriittisen infrastruktuurin suojaaminen Suomessa. Kandidaatin tutkielma, Jyväskylän yliopisto.

Laiho M. (2020). Toimenpidealoite yhteiskunnan toiminnan kannalta kriittisten alojen työntekijöiden tai sen määrittelyjen perusteiden säätämiseksi. Toimenpidealoite TPA 27/2020 vp, Suomen eduskunta.

Lehto M. (2013). The cyberspace threats and cyber security objectives in the cyber security strategies. *International Journal of Cyber Warfare and Terrorism*, 3(3):1-18.

Lehto M. (2015). Phenomena in the cyber world. In M. Lehto and P. Neittaanmäki (eds.), *Cyber Security: Analytics, Technology and Automation*, pp. 3-29. Springer, Cham. Doi: 10.1007/978-3-319-18302-2_1.

Lehto M. (2020). Cyber security in aviation, maritime and automotive. In P. Diez, P. Neittaanmäki, J. Periaux, T. Tuovinen, and J. Pons-Prats (eds.), *Computation and Big Data for Transport*, pp. 19-32. Springer, Cham. Doi: 10.1007/978-3-030-37752-6_2.

Liaropoulos A. (2010). War and ethics in cyberspace: Cyber-conflict and just war theory. In *Proceedings of the 9th European Conference on Information Warfare and Security (Thessaloniki, 2010)*, pp. 177-182.

Lobel M. (2014). Security risks and responses in an evolving telecommunications industry. PwC (network of member firms of PricewaterhouseCoopers International Limited).

Loukas G., Gan D., and Vuong T. (2013). A review of cyber threats and defence approaches in emergency management. *Future Internet*, 5(2), 205-236. Doi: 10.3390/fi5020205.

Macola I.G. (2020). The five worst cyberattacks against the power industry since 2014. Power Technology, https://www.power-technology.com/features/the-five-worst-cyberattacks-against-the-power-industry-since2014/

Mallon S. (2020). Ransomware and the defense industrial base. SmartData Collective, https://www.smartdatacollective.com/ransomware-and-defense-industrial-base/

NCC (2019). Cyber security in UK agriculture. NCC Group, https://research.nccgroup.com/wp-content/uploads/2020/07/agriculture-whitepaper-final-online.pdf

NIAC (2017). Securing cyber assets: Addressing urgent cyber threats to critical infrastructure. The President's National Infrastructure Advisory Council (NIAC).

Nikander J., Manninen O., and Laajalahti M. (2020). Requirements for cybersecurity in agricultural communication networks. Computers and Electronics in Agriculture, 179:105776.

OAGOV (2020). Cyber security threats against global governments increase exponentially. Open Access Government, https://www.openaccessgovernment.org/cyber-security-threats-global-governments-increasing/96789/

Okupa H. (2020). Cybersecurity and the future of agri-food industries. Master's thesis, Kansas State University.

Orr K. (2020). Cyber attacks against state and local governments surge. CyberArk Software Ltd., https://www.cyberark.com/resources/blog/cyber-attacks-against-state-and-local-governments-surge

Pagliery J. (2015). The inside story of the biggest hack in history. CNN Business, https://money.cnn.com/2015/08/05/technology/aramco-hack/

Pagliery J. (2016). Hackers destroy computers at Saudi aviation agency. Cable News Network (CNN), https://money.cnn.com/2016/12/01/technology/saudi-arabia-hack-shamoon/

Papesh J. (2019). When tech is the target: Cyber risks for tech companies. AXA XL, https://axaxl.com/fast-fast-forward/articles/when-tech-is-the-target_cyber-risks-for-tech-companies

Police1 (2017). 9 cyberattacks that threatened officer safety and obstructed justice. Police1, Lexipol, Frisco, TX, https://www.police1.com/cyber-attack/articles/9-cyberattacks-that-threatened-officer-safety-and-obstructed-justice-dCWXReoa54CkcH3y/

Polityuk P., Vukmanovic O., and Jewkes S. (2017). Ukraine's power outage was a cyber attack: Ukrenergo. Reuters, https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA

Pye G. and Warren M. (2011). Analysis and modelling of critical infrastructure systems. In *10th European Conference on Information Warfare and Security (ECIW 2011)*, pp. 194-201. Academic Conferences, Reading.

Quinn C. (2018). The emerging cyberthreat: Cybersecurity for law enforcement. Police Chief Magazine, https://www.policechiefmagazine.org/the-emerging-cyberthreat-cybersecurity/

Safety4Sea (2018). 2018 highlights: Major cyber attacks reported in maritime industry. Safety4Sea, https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry/

SCF (2020). All you need to know about cyber security threats in energy sector. Swiss Cyber Forum, https://www.swisscyberforum.com/all-you-need-to-know-about-cyber-security-threats-in-energy-sector/

Scheuermann J.E. (2017). Cyber-physical attacks on critical infrastructure: What's keeping your insurer awake at night? K&L Gates, https://www.klgates.com/Cyber-physical-Attacks-on-Critical-Infrastructure--Whats-Keeping-Your-Insurer-Awake-at-Night-01-24-2017

Securicon (2019). What's the difference between OT, ICS, SCADA and DCS? Securicon, Alexandria, VA, https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/

Spiegel (2014). Hacker legten deutschen Hochofen lahm. Spiegel, https://www.spiegel.de/netzwelt/web/bsi-bericht-hacker-legten-deutschen-hochofen-lahm-a-1009191.html

Stoye E. (2019). Hexion, Momentive and Norsk Hydro all hit by ransomware cyber attacks. Chemistry World, https://www.chemistryworld.com/news/hexion-momentive-and-norsk-hydro-all-hit-by-ransomware-cyber-attacks/3010328.article

Swivel (2020). 9 reasons why healthcare is the biggest target for cyberattacks. Swivel Secure, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/

Synack (2020). The 2020 trust report: Measuring the value of security amidst uncertainty. Synack.

Thompson M. (2016). Iranian cyber attack on New York dam shows future of war. Time, https://time.com/4270728/iran-cyber-attack-dam-fbi/

Tunggal A.T. (2020). What is an attack vector? Common attack vectors. UpGuard, https://www.upguard.com/blog/attack-vector

UN (2018). The protection of critical infrastructures against terrorist attacks: Compendium of good practices. United Nations.

US-Army (1995). Joint doctrine for military operations other than war. Joint Pub 3-07, US Army.

US-GOV (2001). Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) act of 2001. Public Law 107–56, U.S. Congress.

US-GOV (2019). Foreign cyber threats to the United States: Hearing before the Committee on Armed Services, United States Senate, one hundred fifteenth congress, first session, January 5, 2017. U.S. Government Publishing Office, Washington, DC.

van Niekerk B. (2018). Analysis of cyber-attacks against the transportation sector. In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, pp. 1384-1402. IGI Global.

Wandera (2020). Cybersecurity in the healthcare industry. Wandera, https://www.wandera.com/cybersecurity-healthcare/ retrieved 25 January 2021.

Warren M., Pye G., and Hutchinson W. (2010). Australian critical infrastructure protection: A case of two tales. In *SECAU 2010: Proceedings of the 11th Australian Information Warfare and Security Conference*, pp. 30-36. SECAU Security Research Centre.

WaterPower (2019). Hydropower facilities: Vulnerability to cyber attacks. Water Power Magazine.

WEC (2016). The road to resilience: Managing cyber risks. World Energy Council.

Weed A.S. (2017). US policy response to cyber attack on SCADA systems supporting critical national infrastructure. Air University Press.

Williams S. (2020). Tech industry most attacked sector. IT Brief Australia, https://itbrief.com.au/story/report-tech-industry-most-attacked-sector

Yle (2016). Russian group behind 2013 Foreign Ministry hack. Yle, https://yle.fi/uutiset/osasto/news/russian_group_behind_2013_foreign_ministry_hack/8591548

Yle (2020). Emails compromised in cyber-attack on Finland's Parliament. Yle, https://yle.fi/uutiset/osasto/news/emails_compromised_in_cyber_attack_on_finlands_parliament/11716393

Zetter K. (2015). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Broadway Books, New York.