Institute of Information Security

University of Stuttgart
Universitätsstraße 38
D–70569 Stuttgart

Masterarbeit

Critical Infrastructure Security in the Age of Cyberwarfare

Robin Sliwa

Course of Study:	Informatik
Examiner:	Prof. Dr. Ralf Küsters
Supervisor:	Tim Würtele, M.Sc.
Commenced:	December 6, 2022
Completed:	June 15, 2023

Abstract

Our modern critical infrastructure of the 21st century is not only digitized; it is also more interconnected than ever before. While this progress has provided many improvements in efficiency, functionality and maintainability, it also introduced new attack vectors. It subsequently has become a target for coordinated attacks by cybercriminal and government-affiliated hacking groups. Especially current circumstances such as the Russian invasion of Ukraine have made the protection of critical infrastructure a central topic of (inter-)national security.

This thesis provides an overview over critical infrastructure security in the context of cybersecurity. To that end, modern critical infrastructure is introduced and put in the context of legislative frameworks through the lens of European Union regulations. The central part of this thesis explores landmark attacks and incidents in form of Stuxnet and NotPetya. Followed by this, the adversaries behind such attacks and the resources available by them are analyzed; correspondingly, potential countermeasures and paths to enhanced cybersecurity are introduced.

Overall, this thesis finds that critical infrastructure cybersecurity requires a much higher priority by public and private organizations. More than that, it suggests the pursuit of more holistic approaches over isolated measures - and a consideration of cybersecurity implications during all stages of business design and operation.

Contents

List of Figures

Acronyms

ENISA European Union Agency for Cybersecurity. 20

EPCIP European Programme for Critical Infrastructure Protection. 19

IDPS Intrusion Detection and Prevention Systems. 12

NIS Network and Information Systems. 7

NIST National Institute of Standards and Technology. 12

NSA National Security Agency. 38

PLC Programmable Logic Controller. 7

SCADA Supervisory Control and Data Acquisition. 16

1 Introduction

Ever since the dawn of civilization, infrastructure has played a vital role in establishing, growing, and sustaining societies. When it plays a crucial role, we fittingly call it Critical Infrastructure - its presence enables society, while its absence fundamentally threatens it.

In the past decades, our (now global) society and its infrastructure have undergone revolutionary changes, reaching a level of unprecedented interconnectedness. With the rapid digitization of virtually all economic sectors and society as a whole, the underlying infrastructure now provides us with a diverse range of complex services and goods in surprisingly reliable fashion.

However, as we will explore throughout this thesis, this leaves us with the other side of the coin: Our interconnected, digital (critical) infrastructure is not just susceptible to "naturally" occurring disruptions or physical manipulation; it is also a prime target for cyberwarfare. This entirely new avenue of remote attack vectors thus poses new challenges to those seeking to protect it, as attackers have already begun exploiting them.

This thesis aims to gain and give insight into the following questions:

1. What is critical infrastructure, how has it evolved into its modern version we know today, and what does the relating legislative foundation regulating it look like?
2. Have cyberattacks targeting critical infrastructure already occurred, and if so, by whom and why?
3. Which methods and resources are available to these adversaries?
4. What can we do about it?

To do so, we will explore these questions (and the connected topics) over the course of this thesis - which is structured as follows:

Chapter 1 - Critical Infrastructure introduces critical infrastructure and, from a historical context, the role it performs for society. Additionally, we look at the evolution of the European Union's (EU) legal acts pertaining it to establish a general regulatory context.

Chapter 2 - cyberattacks describes landmark cases of cyberattacks that related to Critical Infrastructure and have left an imprint on the cybersecurity landscape until this day; namely Stuxnet and NotPetya. We further take a look at what applied cyberwarfare as part of an open war looks like in form of the Russian invasion of Ukraine since 2022. We then explore the distinct types of adversaries within our context, how they function, and what drives them.

Chapter 3 - Methods and Resources gives an overlook over prominent methods and resources adversaries may utilize to conduct cyberattacks; notably we examine Social Engineering as an exploitation of the human factor, and the application of cyberweapons.

Chapter 4 - Countermeasures suggests several approaches available to organizations wishing to improve their cybersecurity. As there are many different options available, we take a closer look at the United States National Institute of Standards and Technology (NIST)'s Cybersecurity Framework as a representative of structured frameworks, investigate countermeasures for Social Engineering, and take a brief look at existing technical interventions like Intrusion Detection and Prevention Systems (IDPS), and legislative advancements that might aid improving cybersecurity through regulatory means.

Chapter 5 - Conclusion and Outlook returns to the questions raised in this introduction, formulating answers, and summarizing the key findings made. As we draw our conclusion, we give an outlook and recommendations of what steps should be taken for a secure and reliable critical infrastructure of the future.

2 Critical Infrastructure

While there is no universally agreed upon definition of “Critical Infrastructure”, it is generally understood as physical and virtual systems as well as assets required to maintain functionality of government and society, in extension the economy as well. Subsequently, its malfunction, absence, or destruction immediately threatens stability, prosperity or security of the affected state and society [Bun21a; Eur22b].

The concrete specifications of which sectors are included within that term are similar, yet they differ by jurisdiction. They revolve around functionality and continuity of government and its services, as well as fulfillment of basic individual needs and fundamental economic infrastructure. For example, Germany defines critical infrastructure as the following sectors:

- Energy
- Health
- Information technology and telecommunications
- Transport and traffic
- Media and culture
- Water
- Finance and insurance
- Food
- Municipal waste disposal
- State and administration

[Bun21b, Section 2.10] [Bun21a]

Some sectors are widely deemed as critical or essential - the energy sector, for example. It encompasses power generation, transmission, and distribution systems with power plants, electrical grids, and oil and gas infrastructure. Disruptions in this sector (i.e., widespread, ongoing power outages) can have cascading effects on other critical infrastructure sectors. A widespread, long-term power outage will, for example cause increasing failures in other sectors like public administration, supply chains (e.g., food), water supply and the entirety of telecommunication. Such critical infrastructure failures therefore highly disrupt the daily lives of individuals [SGO14, p. 71-72].

Water supply and wastewater treatment are analogously critical; the absence of clean drinking water often has life-threatening consequences for the general population.
Other such sectors include healthcare with clinics, medical supply chains or the underlying organizational infrastructure (e.g., patient data, treatment, and insurance management); or more recently, the telecommunication sector providing modern communication and data exchange mechanisms which have become an integral part of our daily lives.

There are numerous examples of incidents causing cascading failures: In 2005, Hurricane Katrina flooded and largely destroyed the city of New Orleans. It caused massive power outages due to storm and flood damages; many parts of the city itself were catastrophically flooded due to dam failures. Water management, transportation, public transportation, medical services, and telecommunication largely failed; subsequently, public order eroded as governance overall failed and national rescue operations only slowly commenced. While Hurricane Katrina, as a natural disaster, certainly qualifies as a rare catastrophic event of a magnitude difficult to prepare for, it is a prime example for critical infrastructure's importance and why its protection is so vital [Mil06].

Modern threats to critical infrastructure are not limited to physical manipulation or natural disasters; cyberattacks have become a new threat to their continuity. Before we explore those in more depth, we will look at the historical development and status quo of critical infrastructure.

2.1 Historic Development

The historical evolution of critical infrastructure (in a wider sense) can be traced back to the early days of civilization during the Bronze Age. Even in those early days, ancient societies built infrastructure such as roads, bridges, and aqueducts to transport and supply goods and people. In the modern era, critical infrastructure has become comparatively much more complex, encompassing a wide range of sectors such as energy, transportation, healthcare, telecommunications, and finance.

Among others, early development and construction of critical infrastructure can be traced back to the Indus Valley Civilization. It existed during from around 7,000 to 600 BCE in modern day India and Pakistan, with its peak around 2,800 to 1,900 BCE. The civilization had a complex system of urban planning, with well-designed roads, buildings, and drainage systems to support these ancient cities, which are thought of to have supplied 30,000 to 60,000 people. The Indus Valley Civilization was further known for advanced water management systems, with well-constructed water supply and a sanitation systems [Ken08, p.722 - 723].

The Romans are also well known for their multi-faceted, deep, and enduring impact on civilization through the present. For example, their advanced infrastructure systems, including the construction of roads, aqueducts, and sewage systems, have been well studied. These systems allowed for complex supply chains spanning a vast empire and ensured a steady supply of food and clean water for an unprecedented population size and density - fueling their dominance throughout centuries [Ass09]. This enabled the ancient city of Rome to reach a peak population of around half a million people

[Sto97]. On the downside, Rome is also a relevant example of how disruption of such (critical) infrastructure destabilizes society[1], making its upkeep and protection vital to their builders' prosperity and survival [Ass09].

After the decline and fall of the Roman Empire, the development of these types of infrastructure faced significant regression in the Western world during the succeeding Medieval period(s). During this time, much of the already existing Roman infrastructure was left to decay. For example, water supply systems resurfaced in the High Middle Ages (c. 1,200 AD) [Mag03, p. 1-6]; in some areas such as wastewater infrastructure, comparable sophistication was regained only after 1,000 years [LB10].

In the Late Middle Ages and towards the early modern period (Renaissance period), the construction of infrastructure accelerated with the rediscovery of ancient knowledge and the acquisition of new scientific and technological knowledge[2]. It enabled the development of new infrastructure such as aqueducts, canals, and dams. One key step was the growth of (increasingly globalized) trade and commerce, which led to the development of transportation infrastructure, such as roads, bridges, and ports. This accelerated progress significantly contributed to the growth and development of European cities and societies as a whole [ABKY93] - again underlining the vital function of critical infrastructure to its respective society.

Throughout modern period, critical infrastructure continued to evolve with the growth of trade, exploration, colonization, imperialism, and the establishment of global empires. The Industrial Revolutions marked a significant turning point; with ever-increasing scientific gains, standardization, industrialization, and mass production establishing or revolutionizing many sectors we today regard as critical (such as electricity, organized health care, telecommunication, etc.) - culminating in the familiar, analog yet complex critical infrastructure of the mid-late 20th century. Fueled by the Digital Revolution of the (late) 20th century, today's Information Age features a globalized society and economy that are built atop information technology [Gro21].
Alongside it, critical infrastructure has been transformed into today's digitized, modern, and interconnected Status Quo.

2.2 Modern Critical Infrastructure

Modern critical infrastructure is characterized by its increasing reliance on technology and digitization, with its operation not only being automated, but programmed[3]. The sectors vary significantly in their level of digitization and cybersecurity preparedness.

[1] Although the Romans experienced and conducted many types of warfare, cyberattacks were admittedly not one of them.

[2] It is also noteworthy that much Ancient knowledge was preserved in the Islamic world and later reintegrated in the Western corpus; this was complemented with the adoption of various innovations from the Islamic Golden Age - such as algebra.

[3] Traditional machinery such as steam engines may be (somewhat) automated, but changes in operational procedure require serious manual intervention and repurposing. In contrast, programmed systems are comparatively easy to adjust in many cases.

2.2.1 Electricity

For example, the electricity sector has evolved from a physical network of interconnected traditional power plants to large smart grids that incorporate advanced sensors and regulate themselves efficiently to maintain optimal operation depending on overall and localized supply and demand. Both demand and supply are highly variable, with the latter being provided by a complex network of power plants, substations, transformers, and distribution lines to deliver electricity efficiently and reliably. The underlying power generation sources range from traditional fossil fuel-based plants to renewable energy installations such as solar and wind farms [BCFD16].

To ensure the stability and resilience of the electricity sector, advanced control systems and monitoring technologies are being used. Supervisory Control and Data Acquisition (SCADA) systems, for example, enable real-time monitoring and control of power generation and distribution processes. These systems collect data from various sensors and devices, allowing operators (or machines) to regulate power flows, respond to rapid fluctuations in demand, and detect and mitigate potential issues [HKMS12].

Both its high digitization and vital role in society, economy and other critical infrastructure sectors make the electricity sector a key asset governments want to supervise, but also a prime target for cyberattacks [HKMS12; KV17].

2.2.2 Healthcare

The healthcare sector has also seen a shift towards digitization. This encompasses the widespread use of electronic health records in clinics and other medical facilities. Whereas patient files, treatment plans and schedules and appointment systems used to be analog both in processes and file storage, today's health infrastructure runs predominantly on digital systems[4] [IIDE22].

Furthermore, the surrounding infrastructure has made a digital transformation as well. Taking Germany as an example, certificates of incapacity[5] are transmitted electronically between medical facilities, patients' statutory health insurance and employers since 2023 [SR22]. In some countries, medical prescriptions are transmitted electronically as well.

Beyond mere digitization, these developments fuel several current trends: The concept of patient centricity defragments their medical data and enables them to get a more harmonized, patient-needs centered medical experience (e.g., through unified patient files). With the related data centricity, vast amounts of patient data have become available e.g., for research or treatment decisions [IIDE22].

This introduces new threats as well: Data breaches potentially expose patients' most private, vulnerable data to whomever gained access to it. Malware attacks, such as the WannaCry ransomware[6], can cause serious service disruptions by rendering the infrastructure unusable; even worse, permanent

[4] Although this can clearly differ from country to country: Technological relics such as Fax machines with paper printouts continue their existence in places like Germany.

[5] A licensed doctor's certificate confirming the patient's inability to work due to illness

[6] Ransomware encrypts a system's files after infection, eventually taking the files or the entire system hostage. It displays instructions for the user to pay a ransom; once the (crypto-) payment is received, it may (or may not) provide the user with decryption instructions.

encryption may provoke unrecoverable data loss. Such incidents have already become a reality, as WannaCry demonstrated in 2017 when it caused significant service disruptions within the United Kingdom's NHS [WHD18, p. 25168].

2.2.3 Transportation - ETCS

The transportation sector has also undergone a digital transformation, with the use of technologies such as GPS, vehicles with varying degrees of automation, and intelligent transportation systems to improve efficiency (i.e., throughput) and safety.
For example, under the direction of the European Union Agency for Railways (ERA), the European Train Control System (ETCS) has been developed as part of the wider European Rail Traffic Management System (ERTMS)[7]. ETCS supersedes the national, largely incompatible legacy systems for controlling and signaling in railway systems and is currently in implementation through multiple pilot projects within the European Union.

Traditional train control systems typically use physical signals, such as colored lights, to convey information to the train driver. In contrast, ETCS relies on a digital signaling system, which is more accurate and reliable. It uses wireless communications between the train and the ground-based equipment, allowing real-time monitoring of train movements and better coordination between trains on the same tracks [DB 18, p. 5-7].
ETCS consists of several "levels", each with increasing levels of functionality and automation. Level 0 provides basic signaling information to train drivers, while Level 1 adds continuous train monitoring and automatic speed control. Level 2 adds real-time communication between trains and trackside equipment, allowing for more precise train control and greater capacity on busy routes[8]. Finally, Level 3 is the most advanced level, with complete automation of train control and no need for trackside signaling equipment [DB 18, p. 7-8].

However, there are concerns about cybersecurity. If the system were hacked or otherwise compromised, it could lead to profound consequences such as service disruptions, train accidents or terrorism-related, lethal collisions. Also, there is a risk of data breaches or unauthorized access to sensitive information stored within the system [LA15].

There have been specific concerns regarding the security of ETCS and the GSM-R network standard, the latter being an adapted version of the general GSM standard (thus inheriting security concerns associated with GSM). With it, handheld devices attempting to connect need to pass a (one-way) challenge-response procedure, and communication is encrypted with a 64-bit key. This allows the keys to be calculated within minutes, allowing traffic decryption or redirection of handheld devices' traffic, and imitation of base stations. Accordingly, the process is already underway to replace GSM-R with a modern successor called the Future Railway Mobile Communication System (FRMCS), to be phased in by 2030 [GBL+18, p. 5].

ETCS itself also has potential attack vectors associated with it. For example, seeking collisions in the used message authentication codes could potentially be used to get the encryption key through the used CBC-MAC algorithm. On the other hand, old messages may be resent to recipients - which

[7] The ERTMS also encompasses GSM-R as wireless communication standard adapted for railways, and the European Train Management Layer (ETML) for payload management; the latter has not been further pursued
[8] This level is currently in implementation as a pilot project in the train network of the Stuttgart region [BBB+23]

they can identify as being resent via the included timestamp, but only after decryption and MAC verification. In respective quantities, this could be used to disrupt availability by increasing the workload of the messages' recipients [GBL+18, p. 6].

2.3 Legislative Frameworks

The vital importance of critical infrastructure to society implies a desire, if not a need, for the public to regulate it. It is therefore no surprise that many countries have passed legislation defining its scope, minimal security standards and other regulatory means to supervise its establishment, maintenance, and continued development, as well as respective enforcement mechanisms.

The United States, for example, has been implementing critical infrastructure protection measures explicitly since the 1998, when President Clinton issued Presidential directive PDD-63 outlining a national program dedicated to its protection. This directive is an early example for recognition of cyber-threats in an increasingly digitized, interconnected critical infrastructure. It followed a growing awareness for its vulnerability upon the 1995 Oklahoma City bombing, a high-fatality terrorist attack. In the wake of the incident, a commission was established to survey measures on better protecting critical infrastructure; the eventual issuance of PDD-63 (which itself references terrorist threats) can be seen as a result of this period of renewed terrorism awareness [Pre97, p. 5, 14] [Cli98, p. 2].

The program identified the issue as a matter of public-private partnership and established goals for federal, state, and local governments as well as private sector entities; it also defined guidelines on how to obtain them [Cli98].
Further legislation(s) followed 9/11, with President Bush revising the program in 2003. With the publication of the NIST Cybersecurity Framework, the U.S. has also provided a thorough framework for organizations to assess and improve their cybersecurity preparedness; it will be discussed in Chapter 5.2.1.

We will explore the regulatory frameworks surrounding critical infrastructure through the lens of the European Union.

2.3.1 Evolution of European Legislation

EU-level legal acts have taken an increasingly central role for protection measures since the 2000s. With those replacing independent national legislation[9], it is a good representative of its class of regulation. The development of EU legislation on the topic temporally aligns with the critical infrastructure's (and society's) digital / technological evolution and corresponding changing regulatory needs. It further displays emerging challenges at adapting to these requirements, especially with a constantly shifting threat landscape. With the exception of a brief exploration of Germany's NIS

[9]While implementation and (to some degree) its specifics remain within the power of national legislatures, EU Directives provide the direction and guidelines that need to be transposed into national law. EU regulations, on the other hands, are immediately binding.

implementation (see Chapter 2.3.2), this thesis refrains from going into detail regarding corresponding national legislation of EU member states, both those implementing EU directives as well as independent national legislation (e.g., those preceding respective EU-level regulation).

It is also important to note that this subsection does not (and cannot) give a complete account of the massive corpus of previous and current EU-level regulations, as this would overextend the scope of this thesis. Accordingly, the key points and developments in legislation are described; they give a suitable overview of the changing regulatory environment in the EU even without completeness.

EPCIP & ECI

In the wake of the March 11, 2004 Al-Qaeda train bombings in Madrid, the European Council requested preparations for an "overall strategy to protect critical infrastructure", which had already become an increasing area of interest in the wake of the September 11, 2001 terror attacks in the United States and the subsequent surge of global terror attacks during the "War on Terror". While The Commission of the European Communities identified cyberattacks on critical infrastructure as an emerging threat and subsequently outlined the creation of a European Programme for Critical Infrastructure Protection (EPCIP) [Com04, p. 3], these plans encompassed measures for a variety of threats. Further consultations led to the eventual establishment of the EPCIP in December 2006.

The EPCIP, as a first EU-wide legislative framework for critical infrastructure, consists of multiple components [Com06a]:

- Identification and designation of critical infrastructure, including common methodology for (re-)assessing the need for improved protection (further specified by directive 2008/114/EC)
- Establishment of EU-wide expert groups and information sharing processes for the protection of critical infrastructure
- Support for member countries for their national critical infrastructures
- Provision of financial means for related measures

During the legislative process of establishing the EPCIP, the European Commission emphasized the need for a harmonized approach to designation and protection of (national) critical infrastructures. This was based primarily on the national critical infrastructures' interconnectedness and interdependency. A consequence of modern European economic practices (i.e., just-in-time and heavily interconnected manufacturing processes), making the single market increasingly vulnerable to the failure of required infrastructure even on a national level [Com04].
Furthermore, the digitization of the underlying critical infrastructure increased reliance on information technologies such as the internet, space-based positioning and navigation[10], as well as communication. This was seen as a potential risk with failure of such systems leading to potentially union-wide cascades. [Com04].

[10]Europe was entire reliant on the US-controlled Global Positioning System (GPS) or the Russian Global Navigation Satellite System (GLONASS). This external dependency has been resolved by the launch of the EU-created Galileo system in 2016 - but the overall dependency on such technology remains.

The defining criteria of European Critical Infrastructure (ECI) (within the scope of this legislation) reflect the changing properties of critical infrastructure within the European Union. In order to qualify as ECI, critical infrastructure [11] must impact at least two member states and do so in accordance with cross-cutting criteria. These are based on the expected severity of casualties, economic effects as well as public effects [Eur08, Art. 2, 3].

Operator Security Plans (OSP) are mandatory procedures that identify the ECI assets and the respective security measures that are - or could be - implemented for protection. Those plans need to cover (at least) the following three aspects [Eur08, Annex II]:

1. Identification of important assets
2. For the identified assets, conduction of a risk analysis with respect to vulnerability to major threat scenarios and their impact
3. Identification, selection, and prioritization of countermeasures both permanent and graduated (activated relative to risk / threat levels)

Furthermore, the legislation established the position of Security Liaison Officers as the "point of contact for security related issues between the owner/operator of the ECI and the relevant Member State authority" [Eur08, Art. 6 Sec. 1].
Overall, the directive emphasized communication and information exchange both between the Commission and member states, and among member states affected by such ECI. For this purpose, it also established rules for regular data reports as well as conduction of regular threat assessments [Eur08, Art. 7].

While the EPCIP laid the groundwork for an EU-level system to protect critical infrastructure, several shortcomings and restrictions were apparent [RH10, p. 42]:

- Only the energy and transport sectors were targeted by the EPCIP - which is only a fraction of overall critical infrastructure (compare with the exemplary list in Chapter 2.)
- The underlying action plan was a Communication from the European Commission - and as such not legally binding
- Much of the focus was put on trust building and information exchange between the relevant stakeholders on EU-, member state-, and infrastructure operator level (instead of binding regulation)

Early Steps on Cybersecurity

On March 10, 2004, the European Union Agency for Cybersecurity (ENISA) was established[12] as an EU-level agency for network and information security[13]. This happened under the context of information systems, computing and (communication) networks achieving ubiquity in the early

[11] Directive 2008/114/EC specifies critical infrastructure as "an asset, system or part thereof [...] essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State[...]"

[12] The temporal proximity to the Madrid bombings (Chapter 2.3.1) is coincidental.

[13] While it was originally named "European Network and Information Security Agency", ENISA was renamed in 2019 to reflect its much expanded responsibilities.

2000s, as the assurance of their availability and security had become an increasing concern. Furthermore, the early 2000s had shown a drastic increase in cybersecurity breaches and resulting damages [Eur04, Pmbl.].

The new agency's initial purpose was defined as the facilitation of a high and effective level of network security, and to foster a culture around those goals. Accordingly, ENISA's objectives included the acquisition of high expertise. They further encompassed raising awareness and promoting cooperation between stakeholders in the public and private sectors. To achieve those goals, it advised the Commission, member states and businesses on those matters and functioned as an advisor to the Commission for further legislative action based on its assessments [RH10, p. 44]. Its responsibilities and scope were - and are still being - expanded over the years, as we will discuss in more detail later.

In 2009, the Commission presented a Communication on Critical Information Infrastructure Protection (CIIP), building on earlier measures such as the establishment of ENISA and the introduction of the EPCIP as an EU-level definition and security approach to Critical Infrastructure (see Chapter 2.3.1). Further preceding measures included the 2006 "Strategy for a secure information society" to establish a coordinated strategy for the pre-existing initiatives, as well as the various affected stakeholders.
To that end, the Commission proposed measures regarding intensified (multi)-stakeholder dialogue, improved data collection, and a European sharing and alert system for improved response, and suggested actions for the member states to take. The strategy also encouraged private sector stakeholders to take initiatives improving awareness of their security needs and risks [Com06b]. However, this strategy had not been seen as achieving sufficient ownership and implementation by the relevant stakeholders [Com09, Pmbl.], underlining the need for further regulatory attention.

The 2009 Communication recognized the threat and danger of large-scale cyberattacks in the wake of an increasing number of incidents, including its member states Latvia and Estonia. In the latter case, many Estonian institutions such as parliament, ministries, banks, and media outlets were targeted with Distributed Denial of Service (DDoS) attacks through their websites; many of those targets qualify as critical infrastructure. These attacks had occurred in 2007 in conjunction with a diplomatic dispute between Estonia and Russia regarding the relocation of a Soviet-era World War II war memorial and graves, with Russia being accused of orchestrating the incidents. At the time, this was seen as the first potential occurrence of cyberwarfare conducted by one country against another. Ultimately, there was no consensus over Kremlin responsibility [Tra07]. In retrospect, the later occurrence of similar DDoS attacks against Georgia in conjunction with its invasion of the country in 2008 have led some to reevaluate the incidents in context of emerging Russian cyber-operations over the years [Gre19].

In order to improve protection of the information and network systems, the Commission proposed actions to "complement existing and prospective measures in the area of police and judicial cooperation to prevent, fight and prosecute criminal and terrorist activities targeting ICT[14] infrastructures"[Com09, Sec. 2].

[14]ICT stands for "Information and Communication Technology", a term used by the European Commission

To that end, the Commission lined out five "pillars" on how to address the uneven, uncoordinated, and insufficient existing measures [Com09, Sec. 4][15]:

1. Preparedness and prevention: to ensure preparedness at all levels
2. Detection and response: to provide adequate early warning mechanisms
3. Mitigation and recovery: to reinforce EU defense mechanisms for Critical
4. International cooperation: to promote EU priorities internationally
5. Criteria for the ICT sector: to support the implementation of the Directive on the Identification and Designation of ECI

Furthermore, evaluation of introduced actions and the overall current state were scheduled by the end of 2010. Among other reasons, this served as a baseline for the general debate on the future of the EU's policy on the matter [Com09, Sec. 6].

2013 Cybersecurity Strategy

In 2013, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy in a Joint Communication released the Cybersecurity Strategy, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

It built on the 2009 Communication (Chapter 2.3.1) on CIIP. As such, it continued to emphasize the importance of a comprehensive approach to cybersecurity, building upon the 2009 Communication's framework. It called for the creation of a European Cybersecurity Strategy intended to provide a unified approach to cybersecurity across the European Union. It aimed to enhance the EU's preparedness and resilience to cyber threats, foster cooperation and information sharing among stakeholders, and promote the EU's global leadership in cybersecurity.
To reach these goals, it lined out five main priorities [Eur13b]:

1. Achievement of cyber resilience[16]
2. Drastic reduction of cybercrime
3. Development of cyberdefense policy and capabilities, in relation to the Common Security and Defence Policy (CDSP)
4. Development of industrial and technological resources for cybersecurity
5. Advancing international cooperation and coherent policy on cybersecurity

To address these outlined priorities, the following measures were proposed:

To achieve cyber resilience, which involves building the capability to withstand and respond to cyber threats, the EU further updated the roles, capabilities, and responsibilities of ENISA, which provides expertise and support to member states in the area of cybersecurity.

[15] The five pillars are a direct excerpt from the Communication
[16] In this context, cyber resilience describes the ability of entities to continue operation despite cyberattacks

It also called for further work on NIS security and adoption of a proposal for the NIS Directive to regulate "national capabilities and preparedness, EU-level cooperation, take up of risk management practices and information sharing on NIS" [Eur13b, p. 7].

This was eventually implemented via the 2016 NIS Directive, which requires member states to adopt national strategies for cybersecurity, establish a computer security incident response team (CSIRT), and report major cybersecurity incidents (see Chapter 2.3.2). A larger revision, "NIS2", has been passed in late 2022 to further develop these goals relating to NIS security (see Chapter 5.4.1).

To achieve a "drastic reduction of cybercrime", the Commission emphasized the need for fast and thorough legislative implementation regarding cybersecurity in its member states (directives, treaties), strengthened operational capabilities through improved national cybercrime units, and further EU-level cooperation and harmonization [Eur13b, p. 9].
Towards improving the operational capabilities and cooperation, the EU had already established the European Cybercrime Centre (EC3), which is part of Europol and serves as a central hub for cybercrime investigations, intelligence gathering, and operational support to member states [Eur22c]; the Commission committed to working closely with it - as well as Europol (and Eurojust) - to "align such policy approaches with best practices on the operational side". Overall, the EC3 was given a leading role as the European "focal point in the fight against cybercrime" [Eur13b, p. 10].

The desired development of cyberdefense policy and capabilities related to the Common Security and Defence Policy (CSDP)[17]. The EU recognizes cyberspace as a domain of conflict, and as such, has declared cybersecurity an integral part of its security and defense policies. It has been working to develop a coordinated approach to cyber defense, including the creation of a "Cyber Defence Centre", the establishment of a Cyber Defence Rapid Response Team, and the development of a Cyber Defence Policy Framework. For that purpose, the High Representative focused on and encouraged further dialog with the EU's partners, including the North Atlantic Treaty Organization (NATO), to cooperate and complement cyberdefense efforts, but also to avoid their duplication [Eur13b, p. 11-12].

Towards its fourth priority, the strategy called for (better) developing the industrial and technological resources for cybersecurity under the vision of a Single Market[18] for cybersecurity products. This involved promoting public-private partnerships, investing in research and development, and supporting startups and small and medium-sized enterprises in the cybersecurity industry. The EU subsequently moved to financially promote trusted IT solutions through Contractual Public-Private Partnerships (cPPP) and established the European Cyber Security Organisation (ECSO), initially as an organization to implement the cPPP as the Commission's contractual partner. Today, ECSO is a "European cross-sectoral and independent membership organization for cybersecurity that gathers and represents European public and private cybersecurity stakeholders and fosters their cooperation" [Eur23a]. Further efforts have been placed on promoting the development of European cybersecurity standards and certification schemes[Eur13b, p. 12-14].

[17]The CDSP is a component of the EU's foreign and security policy, which aims to enhance the Union's capacity to respond to crises and contribute to international peace and security. The CSDP encompasses a range of civilian and military missions, operations, and activities, including conflict prevention and resolution, crisis management, and capacity building.

[18]This is in reference to the European single market, an area of all EU member states as well as certain non-members; in it, common rules and standards enforce free movement of goods, capital, services and people.

The fifth and last priority focused on establishing a coherent international cyberspace policy for the European Union and using it to promote core EU values. This involved promoting the development of international norms and standards on cybersecurity, supporting international capacity-building efforts, and engaging in dialogues with international partners to promote cybersecurity cooperation. The EU has been active in promoting international cooperation on cybersecurity issues, including through its engagement with the United Nations, the Organisation for Economic Co-operation and Development (OECD), and the Council of Europe. The EU has also aimed at promoting its self-asserted core values (such as the rule of law, human rights, and democracy) in its international cybersecurity policies [Eur13b, p. 12-14].

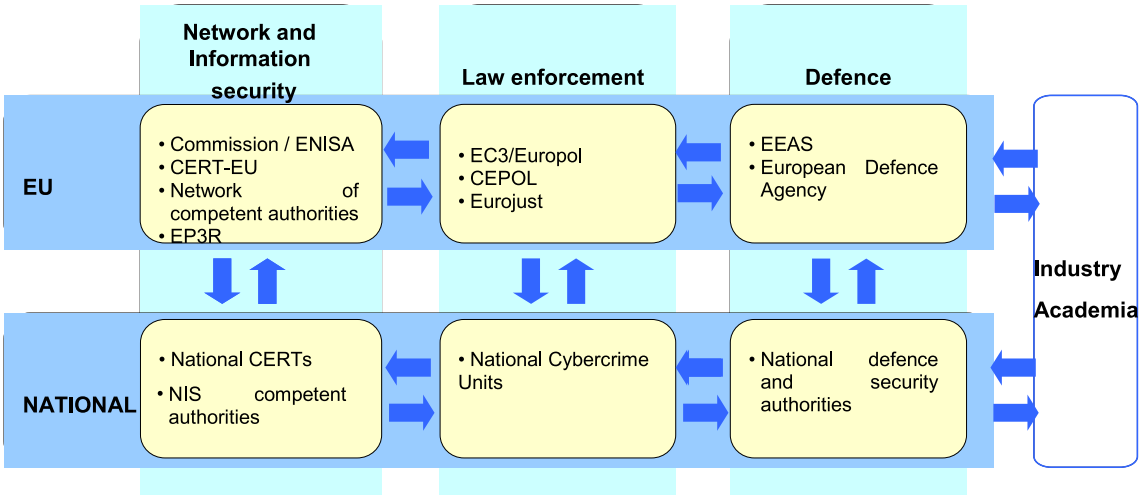


Figure 2.1: Model of NIS-related coordination between EU-level and national authorities in the NIS sector, law enforcement and defense sectors. Image source: [Eur13b, p.17]

Overall, the strategy emphasized the importance of collaboration among all stakeholders to achieve these goals, including government agencies, the private sector, and individuals. These intensified coordination efforts are illustrated in Figure 2.1, displaying information exchange in multiple dimensions, not just between the EU-level and respective national authorities. The coordination is also cross-sectional and includes NIS-related entities as well as law enforcement and defense. Finally, coordination also reaches outside the public sector and connects to the private sector and academia (through aforementioned public-private partnerships and R&D stimulation).

There also were several areas of criticism for the Cybersecurity Strategy, for example:

- Lack of concrete action plans and timelines: Some critics argued that the strategy was too broad and lacked specific, actionable steps to address cybersecurity threats. For example, the European Court of Auditors criticized the strategy in a 2019 report, stating that the absence of measurable objectives hindered not only thorough (quantitative) evaluation but also concrete action in respect to the strategy "expressing rather a vision than a measurable target" [Eur19a, p. 17].
- Overemphasis on public-private partnerships: The strategy's focus on public-private partnerships (PPPs) could lead to a lack of accountability and transparency. This is accompanied by questions over overall efficacy and conflicting interests, as the private sector may prioritize efficiency and profit over the public's interest in security [CB17, p. 1266].

- Lack of attention to privacy and civil liberties: Some privacy advocates criticized the strategy for not adequately addressing the protection of privacy and civil liberties in the context of the strategy's priority of reducing cybercrime [Hus13, p. 6]. Issues within taxonomy - i.e., the definitions for cybercrime, cyberdefense and cyber resilience - were also seen as problematic, since these terms are used for justification of measures interfering in fundamental rights such as privacy and data protection [Hus13, p. 7].

Despite these criticisms, the 2013 Cybersecurity Strategy also gathered positive reception. It was also acknowledged that it was "particularly representative of the push" towards increased coherence of such legislation on the EU-level that had begun in 2013 [CB17, p. 1260].

The NIS Directive, whose initial draft was published in connection to the Cybersecurity Strategy[Eur13a] and eventually adopted in 2016, addressed some of the criticisms of the overall Cybersecurity Strategy by providing more specific and detailed requirements for cybersecurity measures.

2.3.2 NIS Directive

Directive 2016/1148 - more commonly referred to as the NIS Directive - was the first horizontal[19] EU-level legislation dedicated to the security of information and network systems. While the ever-growing importance of such technologies to modern society and its (critical) infrastructure was not a particularly recent insight[20], the process of finally enacting such legislation has been long.

Throughout its 27 articles, the NIS Directive introduced a comprehensive framework that requires member states to identify and designate Operators of Essential Services (OES) and Digital Service Providers (DSPs) in various critical sectors like energy, transportation, healthcare, and finance. Those entities were mandated to ensure the security of their networks and information systems and quickly report significant incidents to their respective national authorities [Eur16].

One aspect that distinguishes the NIS Directive from its predecessors was its emphasis on critical infrastructure sectors and the recognition of the deep and intricate interdependencies between them. By promoting collaboration and information sharing between member states, the directive aimed to bolster the overall resilience and response capabilities across the union. Additionally, it underscored the significance of risk management, incident response planning, and continuous monitoring to proactively identify (and mitigate) arising cybersecurity threats. Accordingly, the legislation once more expanded ENISA's mandate and responsibilities [MPD19, p. 8-9] [Eur16].

It also set forth minimum security requirements and incident notification obligations, fostering a cooperative mechanism among member states for sharing best practices, threat intelligence information, and the conduction of joint exercises. Notably, the directive facilitated the establishment of Computer Security Incident Response Teams (CSIRTs) in each member state, thereby promoting effective coordination in responding to incidents [MPD19, p. 2-4].

The NIS Directive can be seen as a rather late response to an already well-known and escalating issue. However, the fact that it allows member states flexibility and time for implementation (again in part due to it being an EU directive, and implementation specifics being left to national

[19] In this context, horizontal indicates the legislation cutting across sectors, encompassing regulation on multiple subjects
[20] For example, the regulation establishing ENISA already acknowledged this in 2004 (see Chapter 2.3.1)

legislation) could be seen as counterproductive, if the EU's ultimate goal is to establish a robust cybersecurity framework. Despite this, the NIS Directive addresses NIS-related cybersecurity problems comprehensively and laid the groundwork for future regulation [MPD19, p. 11].

It is also important to consider the global perspective, as cybersecurity is a critical area of regulatory interest worldwide. China and the United States have already implemented their own cybersecurity regulations, and data localization remains a contentious international issue. Therefore, the NIS Directive should be viewed as one piece of a larger global puzzle, representing the EU's initial contribution to this complex field, with the prospect of further development and intensified collaboration in the future [MPD19, p. 11].

The 2019 Cybersecurity Act and the recently passed NIS2 Directive (2022)[21] have built upon the foundation laid by the NIS Directive and addressed some of its shortcomings. The Cybersecurity Act established the European Cybersecurity Certification Framework, aiming to enhance trust and security in digital products and services. It further introduced a more harmonized approach to cybersecurity certification, promoting consistency and interoperability across the EU [Eur19b].

Additionally, the NIS2 Directive aims to further strengthen the EU's cybersecurity framework by introducing updated measures based on "lessons learned" and evolving threats. It seeks to enhance the resilience of critical infrastructure, improve cooperation among Member States, and adapt to emerging technologies and risks. These developments build upon the groundwork and experiences gained from the NIS Directive, providing a more comprehensive and robust framework for addressing cybersecurity challenges at the EU level [Eur22a].

Implementation in Germany

Taking Germany as an example for integration of the EU directives into the national legal corpus, NIS was implemented by the Act implementing the NIS Directive[22] in June 2017. Besides implementing NIS, this law expanded the role of the Federal Office for Information Security (BSI) with a supporting role in fostering cooperation between the federal states (and itself), as well as providing advise [Bun22].

The 2015 Act on increasing the security of IT systems[23] had already introduced provisions later reflected by NIS - for example, it made new requirements for operators of critical infrastructure, e.g., in form of mandatory periodic audits or incident reporting in case of possible effects on the availability of essential services [Bun16, p. 7].
The expanded role of the BSI can be seen as somewhat similar to what ENISA represents on the EU level, both in terms of historic evolution of responsibilities (continued expansion) and its role in the provision of cybersecurity (coordination between states, provision of expertise and overseeing mandatory regulations).

[21] We will explore NIS2 in depth in Chapter 5.4.1, as NIS2 is still being implemented well into 2024

[22] "Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union"

[23] This act has been revised in 2021

Accordingly, NIS was implemented with consideration and underutilization of these pre-existing structures; as per the BSI, “the only completely new regulations created in Germany were those for digital service providers [Bun22].
It is hence appropriate to see NIS as an attempt to bring member states’ respective activities, regulations, and structures onto a comparable level; with respect to their pre-existing laws and regulations.

Due to the 2022 passage of NIS2, the federal government is currently in the process of revising and adapting national laws and regulations to reflect the updated EU-level provisions; an early internal draft for the respective implementation law has been publicized in April 2023 [24].

[24]The draft may be found at Intrapol.org.

3 Cyberattacks

At its core, critical infrastructure has always been the target of disruption attempts from those wishing to harm the people reliant upon it. As we have discussed, today's infrastructure has become complex, interconnected and widely digitized. Digital attacks - cyberattacks - have accordingly become an increasingly relevant attack vector. It is therefore only logical that such attacks have already occurred.

To obtain a better understanding of said attacks (and subsequently explore appropriate countermeasures), we will both investigate examples of cyberattacks and take a look at the adversaries conducting them.

3.1 Exemplary Incidents

In this section, we will in-depth explore and investigate two landmark cyberattacks - namely Stuxnet in 2009 - 2010, and NotPetya in 2017. Both attacks displayed various novelties in circumstances, execution and targets that made them noteworthy in their own right; thus, they serve as suitable examples of what such cyberattacks might look like.

3.1.1 Stuxnet

In June 2010, a novel computer worm was first identified by Sergey Ulasen, an employee at a Belarusian anti-virus software provider called VirusBlokAda. The malware had been the cause of Blue Screen of Deaths and appeared to easily propagate through the affected Iranian customer's network while evading regular detection measures [Eug11]. Originally dubbed "Rootkit.Tmphider", these were the earliest hints that Stuxnet would turn out to be unusual in many aspects.

Stuxnet rapidly became known to a wider public starting July 16, 2010, when journalist Brian Krebs published a blog post regarding the novel malware [Kre10]. This was accompanied by a DDoS attack on two websites dedicated to the security of industrial control systems, temporarily disrupting one of them. This disruption included the website's mailing list, which had been a line of communication for information on the new threat for affected stakeholders [Gro11].

In order to install malicious software (infection and propagation), Stuxnet utilized exploitation vectors within Windows. It is common for malware to do so, e.g., to attack remotely or using shellcode[1] to escalate privileges without intended authorization. However, Stuxnet utilized five Windows vulnerabilities to implement multiple propagation methods, e.g., via USB devices, flash

[1] Shellcode is a small code fragment (usually machine code) typically used by an attacker to spawn a command shell with escalated privileges, ultimately paving the way for arbitrary code execution.

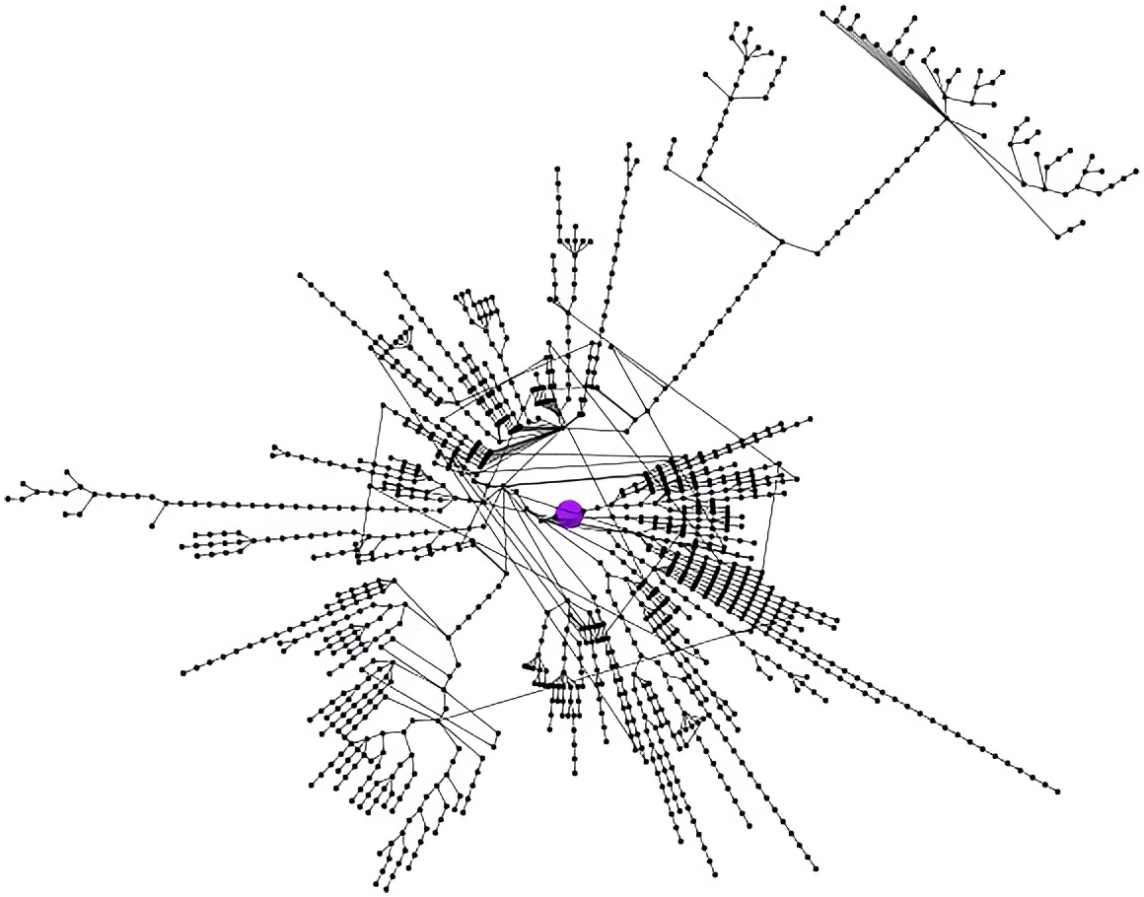


Figure 3.1: Visualization of an infection cluster from the third attack wave in May 2010. Image enhanced via Icons8 Upscaler; original image source: [FMC11, p.8]

drives, or via the network. Four of those were Zero-day exploits previously unknown to stakeholders and as such were initially unpatched on all respective Windows systems. While typical malware might rarely use a Zero-day exploit, the usage of so many of them was considered unprecedented [Fil10]. This, too, indicated the unusual resourcefulness of its creators and their high interest in the success of their malware [MRHM11, p. 7-8].

In most cases, malware design reflects the usual goal of spreading rapidly and uncontrollably to reach maximum impact. Stuxnet was built quite differently, as demonstrated by Figure 3.1. The graph displays an infection cluster originating from an attack initiated on May 11, 2010, with the newer March 2010 variant (see Chapter 3.1.1). The spread of infection can be traced from the initial three infections (purple dot), with each black dot overall representing an infected system. Many branches are primarily linear with a computer propagating only once. This is in stark contrast to typical maximized propagation patterns. Stuxnet behaved this way by design through employment of rate limitation. For example, an infection on a USB drive would intentionally delete itself once three systems have been infected [FMC11, p. 29].

Implementation

The unusual infection and propagation behavior becomes apparent upon analysis of its overall infection routine flow. When its main DLL file - the heart of the malware - is initially loaded, its Export `0x0F` (15) conducts checks on its own configuration data[2] and system compatibility. This process is modeled in Figure 3.2: It will, for example, exit if it detects a 64-Bit operating system or a non-supported Windows version.

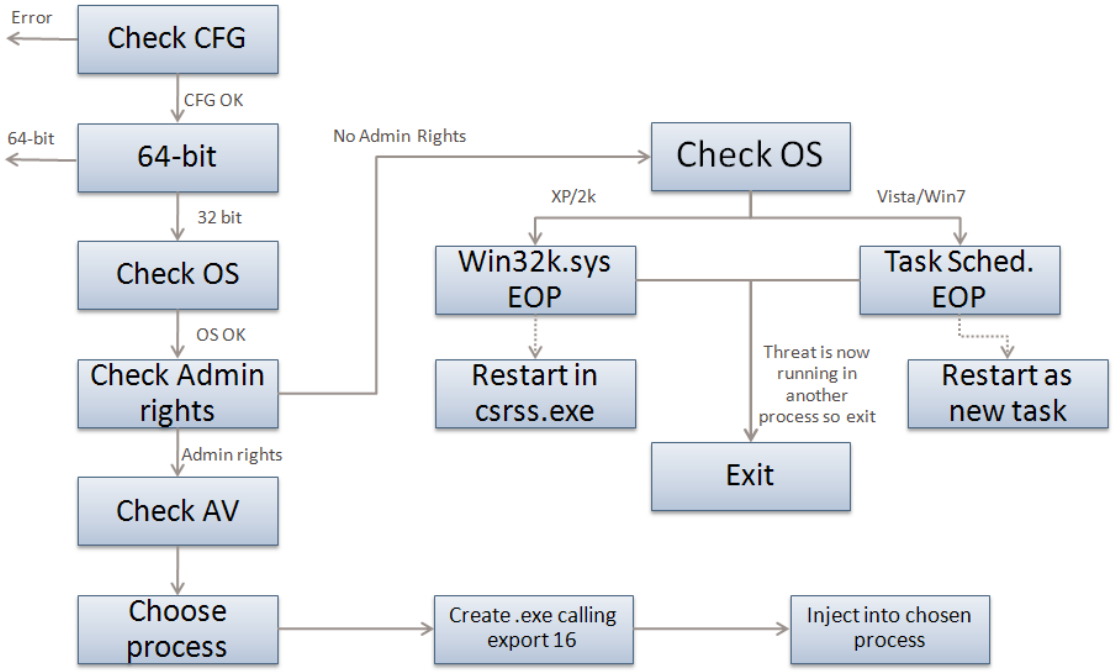


Figure 3.2: DLL Export 15. Image source: [FMC11, p. 16]

The sequence then branches depending on whether it possesses administrative privileges. If it does not, it obtains them by executing one of its Escalation of Privilege (EoP) Zero-day exploits: For Windows Vista and newer (including the corresponding Windows Server products), a Windows Task Scheduler EoP vulnerability[3] is leveraged, eventually leading to a restart as new task with escalated privileges.

For Windows 2000 / XP-era products, it used Kernel-mode driver (Win32k.sys) EoP vulnerabilities[4] related to "the manner in which the Windows kernel-mode drivers maintain the reference count for an object, index a table of function pointers when loading a keyboard layout from disk, and validate window class data" [Mic10]. By doing this, it gets its main DLL loaded in context of `CSRSS.exe`[5], which provides it with the desired privilege level [FMC11, p. 18].

[2]The configuration data contains various flags and information about the respective system and infection state. A full accounting - while outside the scope of this thesis - can be found in [FMC11, Appendix A, Table 13]
[3]This vulnerability was addressed by Microsoft Security Bulletin MS10-092
[4]This was addressed by Microsoft Security Bulletin MS10-073, see [Mic10]
[5]`CSRSS.exe` is the Client Server Runtime Subsystem - its (critical) responsibilities mostly revolve around handling the Windows Console and Graphical User Interface (GUI) shutdown

If administrative privileges are (already) present, it further checks for the presence of antivirus software. Depending on that, it selects its target and injects its main DLL with Export `0x10` (16) being called.

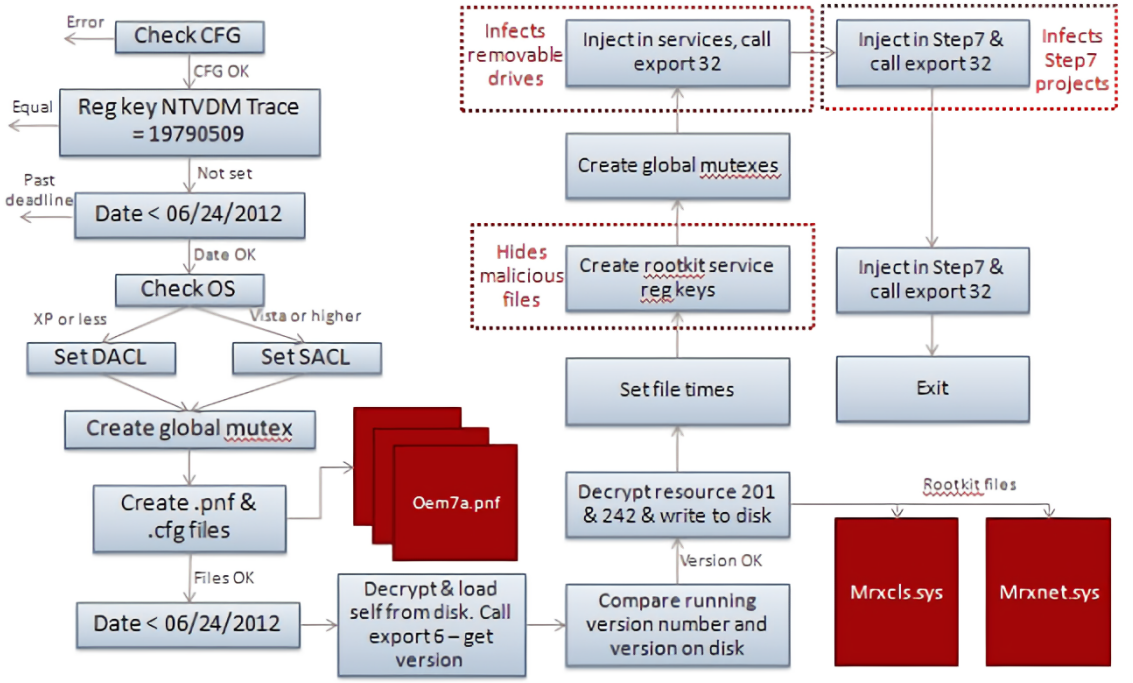


Figure 3.3: Infection routine flow of Stuxnet (DLL Export 16), illustrating the complexity of conditions and exit points for initiation of payload functionality or abort. Image enhanced via Icons8 Upscaler; original image source: [FMC11, p. 17]

Export 16 serves as the main installer. Beyond configuration checks, it again performs multiple checks on how - or whether - to proceed. For example, the malware aborts installation if in the system's registry, the key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MS-DOS Emulation` has its value `NTVDM TRACE` set to `19790509`. This is thought to be a random value[6] serving as a "Do not infect" marker. The malware also checked whether the system date is later than June 24, 2012[7] - a time-based kill switch.

The malware then proceeds to create its (encrypted) files, again checks for the 2012 end date, and proceeds with decrypting and loading itself. Stuxnet then writes its rootkit files (`Mrxcls.sys` loads Stuxnet upon boot and `Mrxnet.sys` used to hide Stuxnet files for infected USB drives [MRHM11, p. 60, 64]) to the disk, performs steps related to hiding itself and proceeds with USB drive infection and performing its main purpose: Infecting project files of a specific Siemens software, STEP 7 (see 3.1.1).

[6]Although likely coincidental, interpreting this value as a date - May 9, 1979 - it aligns with the first firing squad execution of a Jewish citizen - Habib Elghanian - in Tehran after the Iranian Revolution.

[7]It actually checks against a date set in its configuration data, but that has only been observed to have been set to this value

Stuxnet also possesses the ability for updating configuration data. For that purpose, it establishes a HTTP connection to its "Command and Control" (C & C) servers. In analyzed samples, two URLs were identified as such[8]. Upon identification, these domains were redirected to prevent communication; although it was possible for Stuxnet to change these URLs, this had not been observed [FMC11, p. 21].

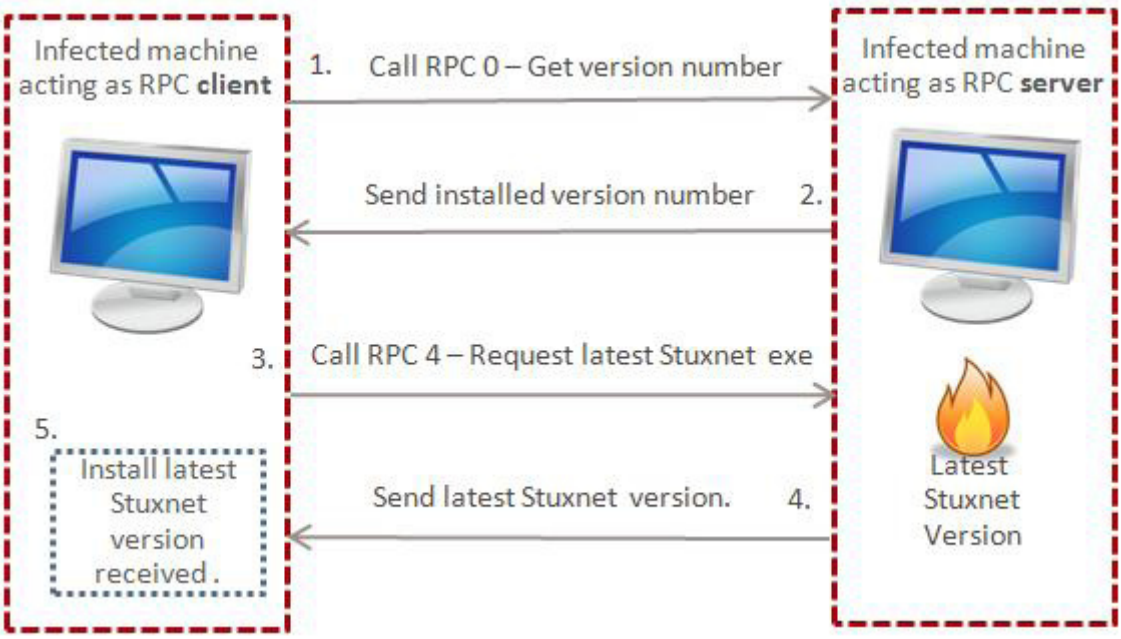


Figure 3.4: Sequence diagram displaying the interaction between two Stuxnet-infected machines, with one acting as RPC server, and the other as RPC client. Image enhanced via Icons8 Upscaler; original image source: [FMC11, p. 25]

It also has the ability to update itself through version comparison of local copies it engages or via the integrated Remote Procedure Call (RPC) functionality. Upon infection, Stuxnet sets up an RPC server with client and proceeds with listening, through which it can communicate in Peer to Peer (P2P) style. Figure 3.4 illustrates an example communication: The client asks and receives the server's version number. In this case, the client's version is superseded by the server's - causing the client to ask, receive and install the newer Stuxnet version. Analogously, if the client's version were newer, the client would send its copy to the server for it to update itself. This mechanism enables the malware to spread updated versions of itself upon introduction (which it did at least twice) [FMC11, p. 25 - 26].

Variants

There exist at least three variants of Stuxnet, which are referred to by their compile times:

- Monday, June 22, 2009; 16:31:47

[8] `www.mypremierfutbol.com` and `www.todaysfutbol.com` from Malaysia and Denmark

- Monday, March 01, 2010; 05:52:35
- Wednesday, April 14, 2010; 10:56:22

Although a fourth variant is thought to exist due to evidence of a changed driver file, the corresponding Stuxnet variant dropping the file has not been observed [FMC11, p. 53].

These variants differ significantly in some respects, especially between June 2009 and March 2010: For example, the March 2010 version has changed components as well as entirely new resources. While some functionality was removed (e.g., Windows 98 support), other functions such as the C&C component were revised - or new functionality added. One major change is the `Mrxnet.sys` rootkit file (used to hide the Stuxnet files on infected USB drives). Where originally, it was an unsigned kernel driver, the March 2010 variant featured an authentically signed `Mrxnet.sys`, with its signature from semiconductor company Realtek, Taiwan [FMC11, p. 53 - 54]. Only after discovery, in July 2010, was the certificate revoked.

An additional version of the driver was discovered with another authentically signed certificate, this time from semiconductor company JMicron, also from Taiwan[9].

Impact and Purpose

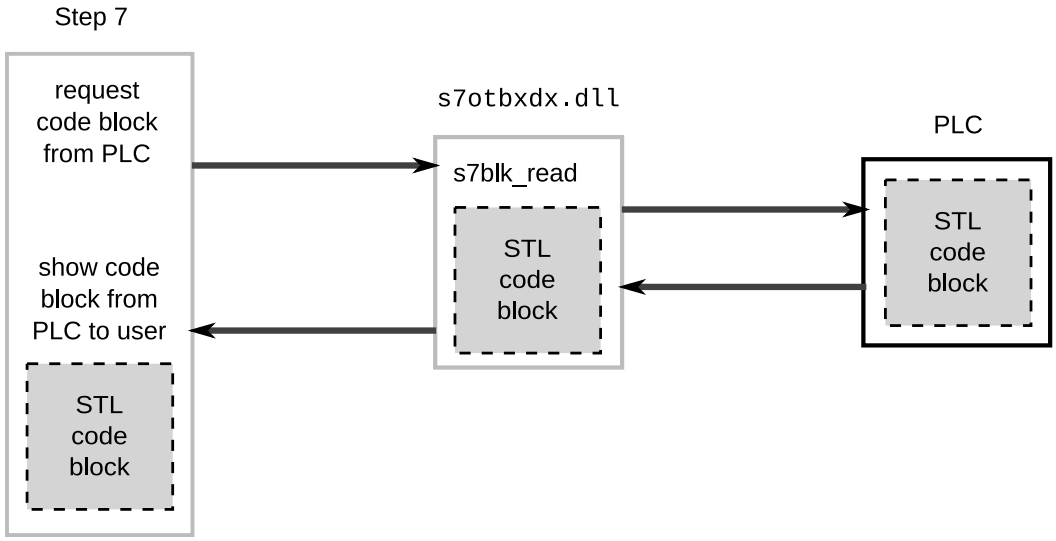
Up until this point, we have looked at Stuxnet predominantly in terms of how its design and overall propagation patterns distinguishes it from typical malware. However, its intended and produced effects were no less remarkable, contributing to its infamous legacy. As discussed, Stuxnet specifically searched and infected project files belonging to a Siemens-made software Suite called "STEP 7".

Siemens' software is used to program and configure an industrial computer hardware type called PLC that is encompassed by the company's SCADA systems. These SCADA systems are used in many environments, including critical infrastructure, such as power plants, water treatment facilities, and oil refineries. By infecting these project files, Stuxnet appears to have been intended to modify the code written to - and being run - on these PLCs.

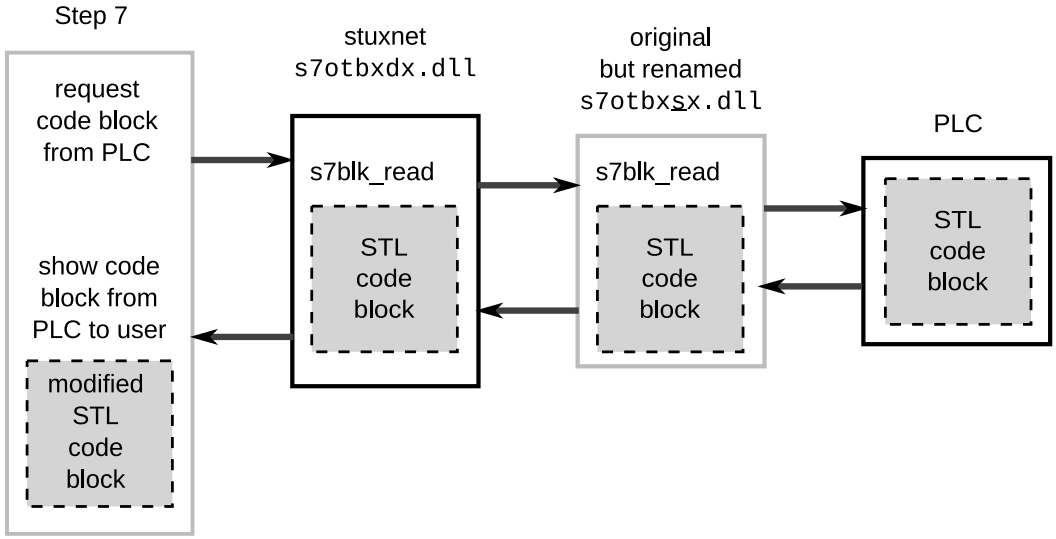
The malware also uses a man-in-the-middle style attack[10] to intercept communication between STEP 7 and the PLC upon their connection via a data cable, as displayed in Figure 3.5. For that purpose, Stuxnet manipulates the software's communication library `s7otbxdx.dll` that may be used to request and read code blocks present on the PLC (see Figure 3.5a). The malware inserts its own `s7otbxdx.dll` in place of the original but keeping the original DLL under another name.
This way, Stuxnet may intercept and arbitrarily modify (or create) any requests by STEP 7 - and do the same for requests returned to it from the PLC, hiding its presence (Figure 3.5b). In fact, Stuxnet provides all exports of the original DLL, with only 16 out of 109 having changed behavior (and the rest being simply forwarded as-is) [FMC11, p. 35-36].

[9] However, this is the driver that had not been observed in conjunction with its corresponding Stuxnet dropper

[10] An attack form where an attacker covertly inserts themselves into communication intended between two parties; they relay and often alter the communication.



(a) Unmodified communication



(b) Stuxnet-modified communication

Figure 3.5: Overview of communication between Step 7 software and corresponding Siemens PLC, with and without Stuxnet-induced modifications. Images under CC BY-SA 3.0; adopted from "Grixlkraxl" (Source: a, b)

Falliere et. al. identified three infection sequences, with Sequence A and B being functional, almost identical, and thus referred to as an overall strategy. Sequence C is seen as more complex, but not functional and incomplete [FMC11, p.37, 45]. However, Stuxnet was very selective about the PLCs that it targeted with its infection sequences: For example, Variants A and B are intended for Siemens' S7-300 CPUs of Type 315-2 in (very) specific setup configurations [FMC11, p. 39]. In contrast, the non-functional Variant C is intended for S7-400 CPUs of type 417 [FMC11, p. 45].

For Variants A and B, Stuxnet looks for specific properties in the device's System Data Block (SDB) with the DWORD at offset `50h` equal to `0100CB2Ch`. This specifies the system uses the Profibus[11] communications processor module CP 342-5. Additionally, Stuxnet searches for specific values, such as `7050h` and `9500h`, which are Profibus identification numbers required for all Profibus DP devices except Master Class 2 devices. These identification numbers are assigned to manufacturers by Profibus and Profinet International for each device type they manufacture. `7050h` is assigned to part number `KFC750V3`, which appears to be a frequency converter drive (also known as variable frequency drive) manufactured by Fararo Paya in Tehran, Iran. `9500h` is assigned to Vacon NX frequency converter drives manufactured by Vacon based in Finland. If the total number of values found is equal to or greater than 33, the SDB check passes [FMC11, p. 39].
The purpose of these specific checks appeared to be the identification of particular machines used in the Iranian nuclear program, so that Stuxnet can target them specifically [San12b].

In the case of the Natanz Nuclear Power Plant in Iran, Stuxnet appears to have altered the speed of the Uranium-enriching centrifuges by subtly slowing or increasing the frequencies at which the centrifuges were spinning. As they need to be operated at very narrow and specific speeds, this alteration likely caused the centrifuges to fail at an increased rate [FMC11, p. 43].
This matches observations by the International Atomic Energy Agency (IAEA), which supervises Iran's nuclear program[12]: About 1000 centrifuges were decommissioned and replaced at the Natanz site in late 2009 to early 2010 [ABW10]. That drop is visible in Figure 3.6, with 3.6a showing the trends of installed as well as UF_6[13]-fed centrifuges at the Natanz size, with a significant reduction appearing around Winter 2009/2010. This is also visible in the plant's operating trends, where the monthly processed amount of UF_6 dropped noticeably (see Figure3.6b) [ABW10].
These observations correlate with both Stuxnet's operational timeframe and code analysis evidence, suggesting a causal link between the two [ABW10; San12b] [Lan11, p. 49].

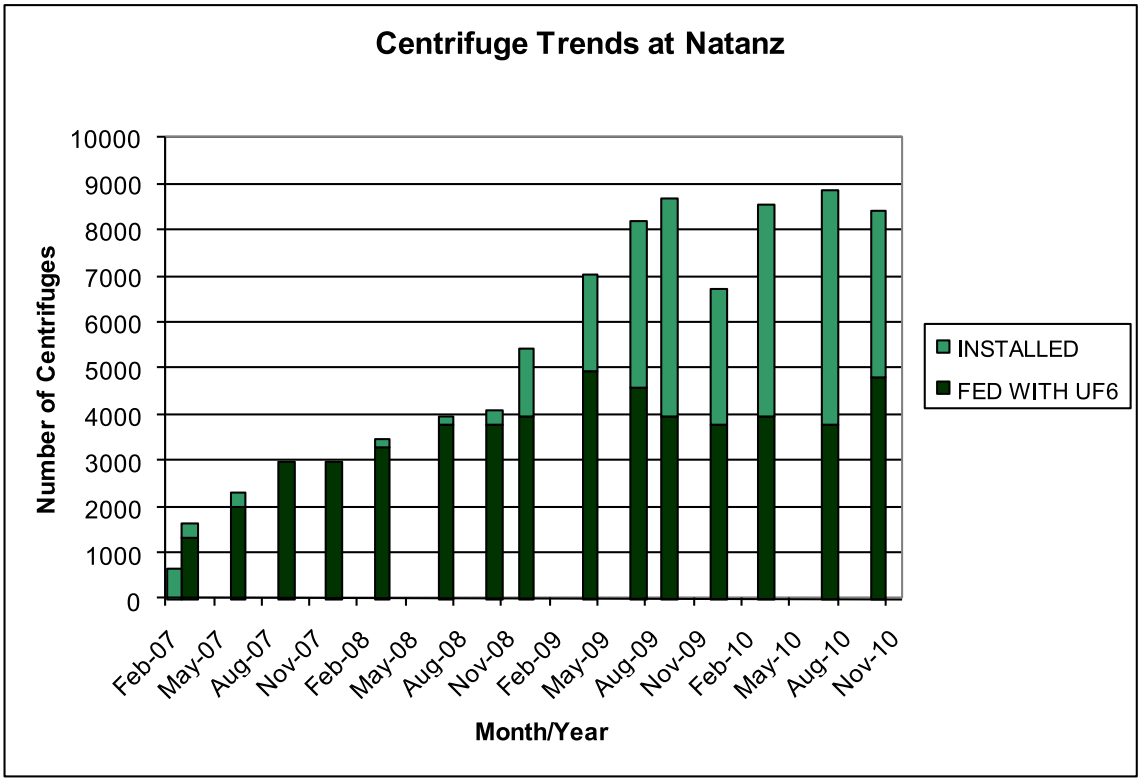
Origins

While both the origin and purpose of Stuxnet are - to an extent - still a matter of debate, it is widely believed that it was created as a government-created cyberweapon to sabotage the Iranian nuclear program [Hal10; San12b].

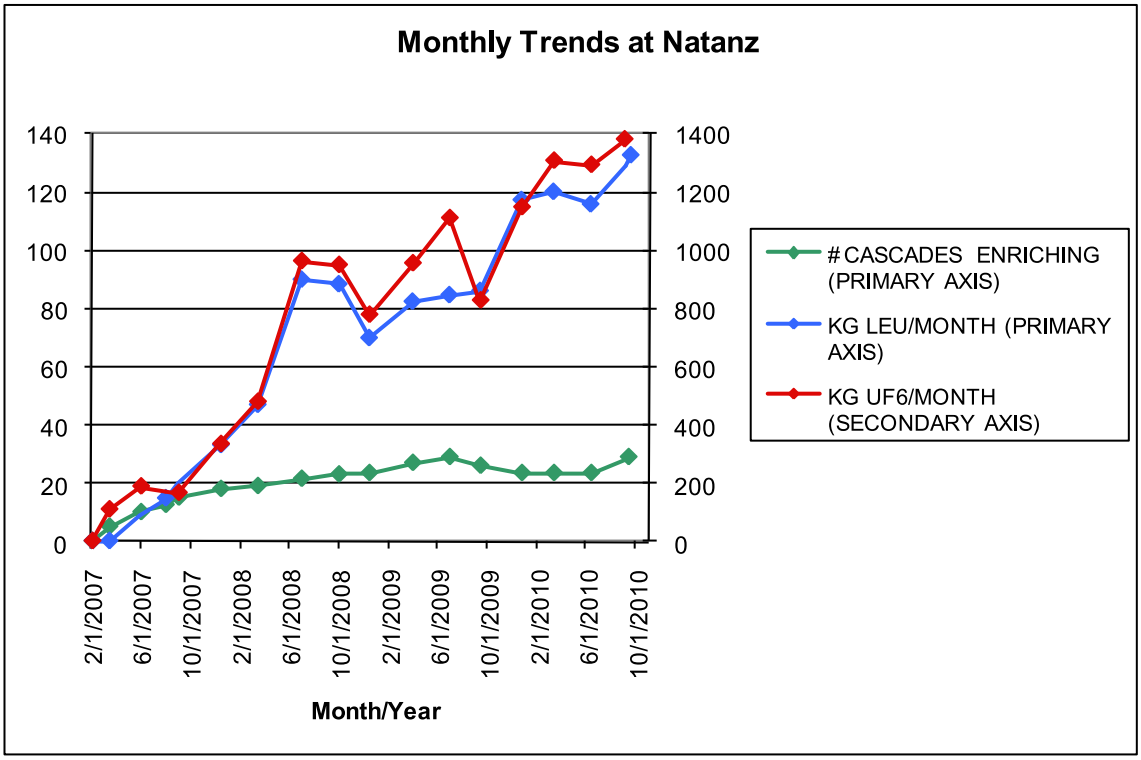
[11] Profibus is a standard industrial network bus used for distributed I/O

[12] It does so to ensure compliance with international regulations intended to prevent - or slow - the creation of nuclear weapons under the disguise of civilian use

[13] Uranium hexafluoride is used for Uranium enrichment, i.e., isolating desired Uranium-235 from the much more common Uranium-238 through gaseous diffusion - or gas centrifuges



(a) Operational centrifuges by month



(b) Monthly operating trends

Figure 3.6: Overview of centrifuge and operational trends at Iran's nuclear site in Natanz from 2007 to 2010. Images adopted from [ABW10, p. 9, 10]

Initial coverage drew the conclusion based on more circumstantial evidence, such as the strong opposition of the U.S. and Israel against Iran's nuclear program, the malware's apparent selective targeting of said program, and the necessary resources required to create such complex and sophisticated malware (including multiple Zero-day vulnerabilities) [Hal10].

In June 2012, an article by US-based journalist David Sanger revealed inside information about Stuxnet in a New York Times article[14], "based on interviews over the past 18 months with current and former American, European and Israeli officials involved in the program, as well as a range of outside experts"[San12b].

In the article, Sanger provides a detailed account of the development and deployment of a cyberweapon, Stuxnet, with the intent of disrupting Iran's nuclear program. The project, code-named *Olympic Games*, was a joint operation between the United States and Israel that lasted for several years and involved a team of skilled programmers, intelligence analysts, and military personnel. According to the Sanger, the origins of Olympic Games can be traced back to the Bush administration, which had become increasingly concerned about Iran's nuclear ambitions. In 2006, the National Security Agency (NSA) and the Israeli intelligence agency, Mossad, began collaborating on a program to sabotage Iran's nuclear facilities using a computer virus. The virus was designed to target specific components of Iran's nuclear infrastructure and cause them to malfunction [San12b] - matching the findings presented in Chapter 3.1.1.

The program was continued and expanded under the Obama administration, which saw cyberattacks as a powerful tool for disrupting Iran's nuclear program without resorting to military action (and subsequently, war). President Obama reportedly took a personal interest in the program and was briefed regularly on its progress. He authorized a series of cyberattacks against Iran's nuclear facilities, which were said to have had a significant impact on the country's ability to produce enriched uranium. The developmental success of Stuxnet was due in part to the sophistication of the virus and the skill of its designers. The virus was programmed to replicate itself and spread throughout Iran's nuclear infrastructure, targeting specific types of equipment, and causing them to malfunction. It was also designed to evade detection by antivirus software and other security measures. For that purpose, Stuxnet was developed, tested, and refined over several years, with input from the team of experts comprised from the NSA, the CIA, and the Israeli military [San12b].

In the summer of 2010, a new variant of Stuxnet escaped from Iran's nuclear facilities and began spreading across the Internet. This was thought to be a result of a coding error in one of the updated variants, causing an engineer's computer to be infected while connected to an infected centrifuge system. Once that computer was later connected to the outside world, the malware - erroneously not recognizing the changed environment - spread to the outside world[15]. Whether the error was made on purpose remained unclear [San12b].

This raised concerns that the virus could be reverse-engineered and used by other countries or hackers to launch cyberattacks against the United States or other targets. The incident also sparked a debate within the Obama administration about the risks and benefits of using cyberweapons, with some officials expressing concerns about the potential blowback and unintended consequences of such operations [San12b].

[14]The article preceded a more detailed account in Sanger's book[San12a]

[15]In the end, this eventual escape and propagation is what likely led to Stuxnet's discovery in the first place.

Duqu, Flame and Gauss

In fact, Stuxnet is not the only malware that is associated with Operation Olympic Games: Duqu, a malware with espionage functionality, was discovered by Kaspersky Labs in September 2011. It features strong similarities to Stuxnet, whose code has been thought to have been "massively re-used" in Flame. Another high-profile connection has been established via Flame's digitally signed Windows driver, which is in close resemblance of Stuxnet's signature abuse [BPBF11, p. 2, 8–10, 38].
Unlike Stuxnet, Duqu appeared to have been aimed at information gathering only, as no Stuxnet-like destructive behavior (aimed at PLCs) had been found [BPBF11, p. 8] [BPBF12, p. 973].

Further malware with apparent connections to Stuxnet were observed later: In May 2012, a malware dubbed Flame was discovered and announced to the public; its functionality revolved around cyber-espionage purposes like recording of network traffic, audio, keyboard inputs and screenshots. Like Stuxnet, it seemed to be directed towards Iran, as the majority of infected devices was located there. It appeared to have been active since 2008 [Lee12].

While initially, Flame appeared unrelated to Stuxnet, subsequent in-depth code analysis by Kaspersky showed near-identical code and the usage of a Zero-day exploit present in both (early) Stuxnet's USB drive propagation mechanism and Flame [Kas12]. This discovery was matched with media reports that Flame had indeed been a joint development of the United States and Israel [NMT12] - like Stuxnet.

Also in 2012, a malware called Gauss was discovered by Kaspersky Lab researchers; it is thought to being based on Flame's code platform. It is similar to Stuxnet and Flame; it too displayed cyber-espionage functionality. Unlike Flame, it also conducted credential theft, e.g., for online banking systems, social networks, or e-mail accounts [BPBF12, p. 986].

Legacy

In conclusion, Stuxnet (both with and without consideration of its "cousins") was a groundbreaking cyberattack that targeted industrial control systems, specifically PLCs, using a man-in-the-middle style attack to subtly manipulate sensor data and alter the physical processes that the PLCs were managing. Its ability to modify the PLCs was particularly worrisome, as it was the first known instance of a worm doing so [Fil10].

It was able to spread using various methods, including network connections and infected USB drives, and subsequently even able to bridge the air gap[16] this way. Thus, even the most secure SCADA systems were not immune to the worm's attack, markedly questioning the efficacy of existing security measures. Its impact on cybersecurity and critical infrastructure cannot be overstated.

[16]Physical separation of systems or network, i.e., an isolated local network without any connections to the outside

3.1.2 NotPetya

Throughout 2017, Ukraine was hit by a series of cyberattacks that targeted critical infrastructure and government institutions. The attacks were attributed to a hacker group known as SandWorm, which is thought to be state-affiliated through ties to the Russian government [Gre18]. They had significant impacts on Ukraine's power grid and other infrastructure, causing disruptions to services and raising concerns about the security of critical infrastructure. It was estimated that by the end of NotPetya's rampage, 10% of all computers in Ukraine had their data irreversibly wiped (in absence of secured backups) [Wak17].

The NotPetya attack started on June 27, 2017, when the Ukrainian government and several businesses (e.g., the National Bank of Ukraine) were hit by a Trojan horse-type malware[17] later dubbed "NotPetya". NotPetya was designed to appear as a ransomware attack, but was effectively a wiper, a type of malware that is designed to permanently destroy data and thus render systems inoperable. It achieved this by leaning on the already existing "Petya" malware (which had been used for ransomware attacks).
As can be seen in Figure 3.7a, it fooled users with a faked CHKDSK[18] screen supposedly repairing the system drive's files, while in truth rendering all files permanently inaccessible (Figure 3.7b). That closely resembled Petya, which had done the same thing. However, unlike Petya, NotPetya did not possess a mechanism for decryption upon payment [Gre18; Uni17].

Behavior

NotPetya was initially distributed through a fake update to the M.E.Doc accounting software widely used in Ukraine. The attackers had gained access to the M.E.Doc servers and used it to distribute the malware to at least several computers. The attack was started at around 10:30 AM on June 27, 2017, via the accounting software's automatic updater `EZVit.exe`. Once the malware was installed on a system, it would spread laterally through the network via two principal attack scenarios, using a combination of methods[19] [Mic17b].

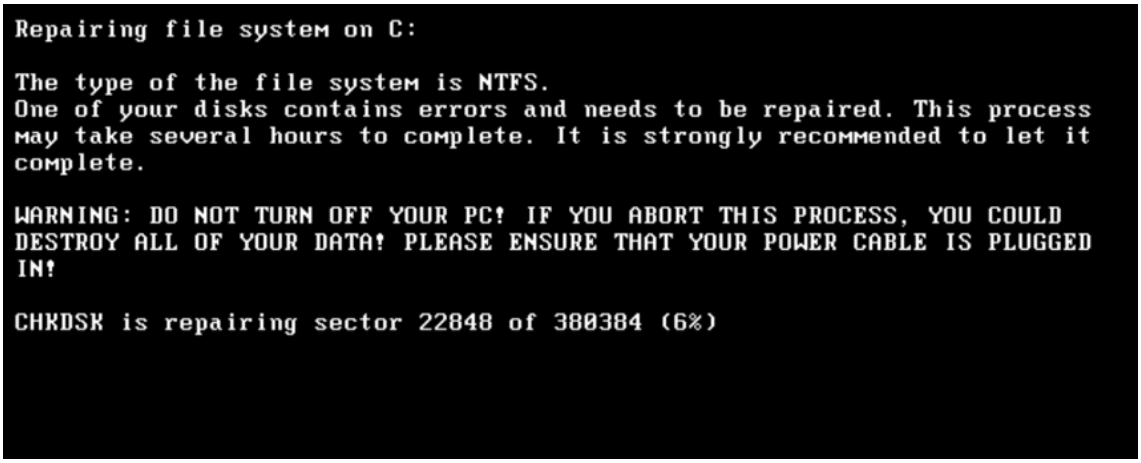
Mechanism 1 - EternalBlue and EternalRomance Exploits The primary method of lateral movement was through the exploitation of the EternalBlue and EternalRomance vulnerabilities first disclosed by the Shadow Brokers group (see Chapter 4.3.1). The exploits allowed unauthenticated remote code execution through specifically crafted SMB(v1) protocol packages used to share files and printers within networks. This mechanism worked on unpatched systems, as the underlying exploits had already been patched a few months earlier [Mic17a; Mic17b].

Mechanism 2 - Credential theft and Impersonation NotPetya was also able to steal and utilize credentials or impersonate users via duplicated tokens. It achieved credential theft by dropping a tool similar to "Mimikatz", which was published in 2011 to demonstrate vulnerable behavior regarding Windows keeping user passwords in memory. As those were accessible, Mimikatz

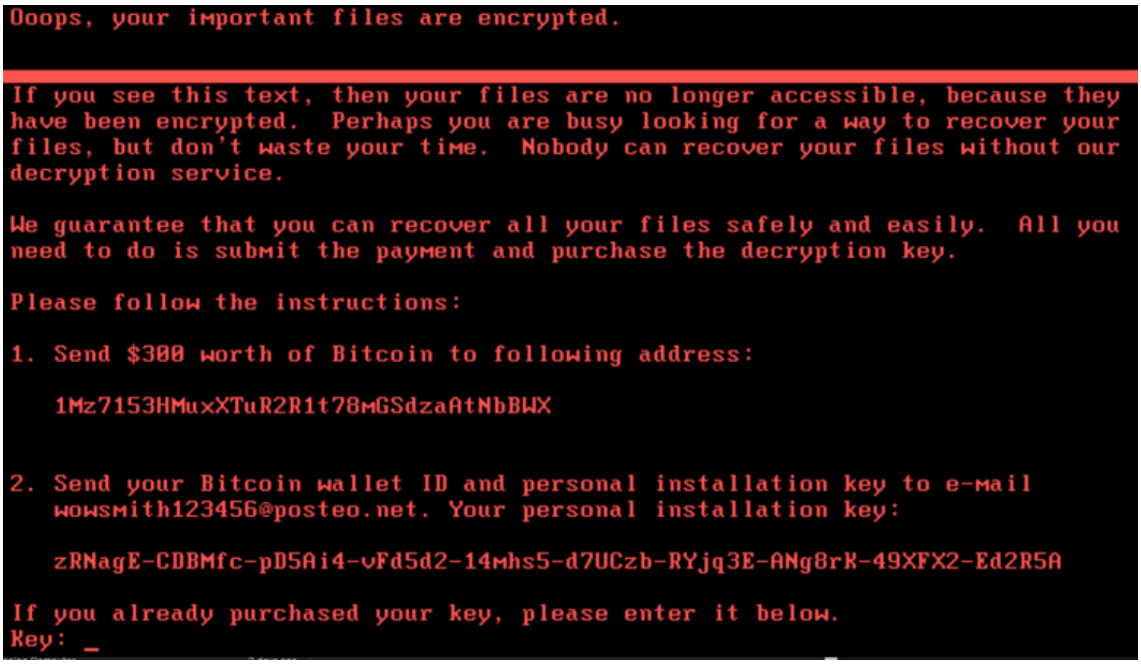
[17] A "Trojan Horse" is, in reference to the ancient Greek myth, a type of malware that infects a system undetected. It tricks the user into downloading, installing, or running seemingly benign software, after which it can execute its malicious behavior.

[18] Check disk - a Windows utility to scan disks and repair their file structure

[19] This maximized spread after initial "seed" infections widely differs from Stuxnet with its strict spread limitations, as discussed in Chapter 3.1.1.



(a) Faux CHKDSK screen during irreversible MFT encryption



(b) Ransomware screen upon reboot

Figure 3.7: NotPetya's displayed messages to the user during MFT encryption - posing as CHKDSK - and afterwards, once rebooted. Those messages closely resembled Petya. Image sources: [SH17]

could recover them. NotPetya used this method to obtain (plaintext) valid credentials from active sessions on the system [Mic17b].
It then scans the local network for available resources, attempts to utilize the stolen credentials, and upon valid authentication, it proceeds with copying and remote executing itself [Mic17a; Mic17b].

Through combination of both attack scenarios, NotPetya was able to spread through systems quickly: Systems not vulnerable to EternalBlue / EternalRomance could still be infected through credentials obtained on those systems that were.

The file encryption would then commence in the background and the system is set up to reboot after a randomly determined amount of time had passed[20] [Mic17b].
The subsequent reboot then leads to the faux CHDKSDK screen (Fig. 3.7a), during which the malware then encrypted the Master File Table (MFT) through the manipulated routines in the Master Boot Record. After the second reboot, it then displayed the ransomware screen (Fig. 3.7b) [Uni17].

Impact and Legacy

While many affected entities suffered from disruptions and subsequent economic damage of varying degrees, several providers of critical functions experienced service disruptions as well - e.g., the Chornobyl Nuclear Power Plant, in Kyiv Oblast, Ukraine. Apart from non-critical functionality such as the website, NotPetya partially disabled site's radiation monitoring system, requiring manual monitoring by staff [Gri17]. Although this did not per se threaten public safety, other disruptions did.

Like "practically every federal agency"[Gre18], The Ministry of Health of Ukraine was also affected. For example, the ministry runs a service that centralizes distribution of medicine among the country's 24 regions. Through it, hospitals can file requests upon shortage; the ministry provides them directly or locates dispensable stock in other regions and sends them to the requestor. The resulting switch to analog fallbacks - i.e., calling every region for every request - significantly increased workload and led to slower response times. At the same time, further health infrastructure services - such as medical document access, were disabled entirely [Bor17].

Yet another critical sector, the financial services, experienced large-scale disruptions. One of Ukraine's largest banks, Oschadbank, had also reported being under attack[21]. Its more than 3000 local branches stayed closed for days, though online banking remained operational [Bor17].
Overall, "more than 22 Ukrainian banks, ATMs and card payment systems in retailers and transport" were disrupted [Gri17], leading to problems withdrawing cash or paying without cash.

In the high-profile case of Danish transport and logistics giant Maersk, the attack started through a computer in Odesa, Ukraine, which had the M.E.Doc tax software installed and served as initial infection. Through the combination of methods discussed earlier (Chapter 3.1.2), the malware rapidly spread across the company's global network, rendering its systems unusable. As recounted

[20] Providing the malware with sufficient time to encrypt files

[21] They did so around 11 AM [Bor17], merely half an hour after the Microsoft-determined start of the attack at around 10:30 AM - again emphasizing NotPetya's rapid spread

by Andy Powell, the company's Chief Information Security Officer (CISO), the network had become impaired within seven minutes, and most of the damage had been done within an hour [Ban19]. Maersk's operations were essentially shut down completely. Without the container tracking software identifying content and routing information, ships were unable to be loaded or unloaded, leading to significant delays in delivery times. This did not only destroy perishable items but also led to cascading effects downstream various supply chains [Ban19].

Most severe of all, the company lost its Active Directory (AD)[22] (domain controller) database; it holds a model of the company's network resources and devices, as well as their relation and organization, among other things. As all backups for the Domain Controller had been (irreversibly) encrypted as well, Maersk did not have a clear and feasible short-term path for recovery of their global, complex network, even with available backups of its business-related data. Through a stroke of luck, a power outage in their Ghana office during the NotPetya rampage led to the discovery of an intact Active Directory database backup a few days later. The system was running again after days, but overall resumption of business activities - including internal communications channels - continued for weeks [Ban19; Gre18].

The attack has been commonly attributed to a hacking group called Sandworm, which is a cyberwarfare unit of the Russian intelligence agency GRU. This attribution has also been made by multiple countries, including the United States, Canada, and the United Kingdom [Gre18; Kov18].
Sandworm has been alleged to have been involved in many hacking incidents, such as an electricity grid attack on Kyiv in 2016 and a 2018 attack on the Winter Olympics during opening ceremonies. Multiple people have been indicted in 2020 for their alleged membership and participation in these cyberattacks [Gre20b].

Despite the attack having been focused on Ukraine, NotPetya caused considerable damage to businesses in other European countries and the United States: About 20% of affected computers were outside of its borders. For example, Maersk individually reported 700 million USD in damages, with the White House estimating the total damage reaching up to 10 billion USD. NotPetya has left an enduring impact as an example for not only how rapid such large-scale cyberattacks can occur, but how deep and cascading the damages might be - a "wake-up call" [Gre18].

For Ukraine, it can be seen as another warning shot in a long series of Russian-attributed cyberattacks that began after the Revolution of Dignity in 2014[23] and continued through the beginning of the Russian Invasion of Ukraine in February 2022 [PT22].

3.2 Russian Invasion of Ukraine

On February 24, 2022, Russian troops launched a large-scale invasion of Ukraine. This open war between the two countries succeeded an almost 8 years period of regional warfare in the Donbas region, predominantly between Ukraine and Pro-Russian separatists covertly supported by Russia.

[22] Active Directory is a Microsoft-developed directory service for Windows domain networks

[23] The Revolution of Dignity describes the series of events leading to the removal of President Viktor Yanukovych, restoration of the country's 2004 constitutional amendments weakening the Presidential powers, and subsequent re-alignment towards the European Union. It was soon followed by the Russian annexation of Crimea and the beginning of the Donbas War.

As we have discussed in Chapter 3.2, this phase of the Russo-Ukrainian war was flanked by Russian-attributed cyberattacks on Ukrainian targets - with the most prominent one being the NotPetya attack in 2017. In this section, we will explore the significance of cyberattacks since the beginning of the invasion and how they compare to pre-invasion incidents.

In February 2023, Google's Threat Analysis Group (TAG) published an analysis of cyber operations associated with the ongoing Russian invasion of Ukraine that began in 2022. While those primarily focus on (Russian) government-associated attackers, those also include associated information operations (i.e., war propaganda). Information operations itself are a long-known method for influencing public opinion both in peace and wartime. Especially Russia's digital mis- and disinformation operations have been in the public eye for over a decade and been discussed in detail. For example, the Russian attempt to influence the 2016 United States presidential election and subsequent large-scale investigations remain a prime example of these activities [Sli20, Ch. 2.2].

The variety of government-backed operations thus encompasses a wide spectrum from limited information operations to actual warfare, and as such, the line between them is blurry at best. For example, the aforementioned Russian election interference qualifies as information operation in form of a disinformation campaign [Sli20, p. 65], while wartime propaganda and disinformation might further qualify for warfare operations intended to destabilize society or otherwise gain an advantage over the enemy. On the other end of the spectrum, digitally sabotaging critical infrastructure qualifies as (cyber)-warfare.

Russian cyberwar(-like) operations through government-affiliated groups started long before the start of the invasion in February 2022 - we have already explored prime examples with NotPetya in 2017 (see Chapter 3.1.2). As per Google's TAG, 2021 showed a significant 250% increase in phishing campaigns directed at Ukrainian users as compared to 2020, likely as a combination of increased focus of attackers towards Ukraine. In 2022, TAG also recorded a 300% increase of Russian phishing campaigns towards users in NATO countries; predominantly however, these were backed by a Belarusian-backed group called Pushcha (which is closely aligned with Russia, as is the Belarusian government) [Goo23, p.5].

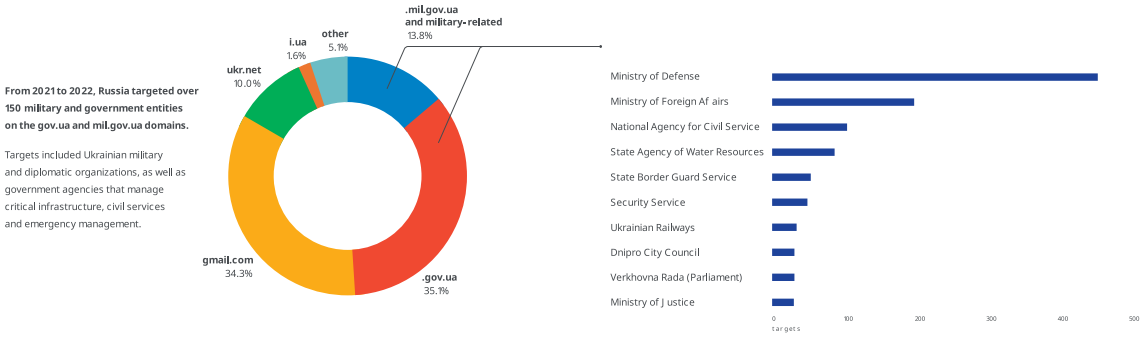


Figure 3.8: Pie chart (left) displaying targets of Russian cyber-activities from 2021 to 2022; to the right, a more fine-grained analysis of the Ukrainian government- and military-associated targets . Image enhanced via Icons8 Upscaler; image source: [Goo23, p.10-11]

These operations before and after the start of the invasion have had a variety of targets. As Figure 3.8 shows, almost half of the targets were military- or government-associated. Among those, the Ministry of Defense was by far the most targeted branch, followed by the Ministry of Foreign Affairs.

Although those are verifiable cyber-operations in a wartime context, there is a notable discrepancy from pre-war expectations. In Chapter 3.1.2, we have discussed the NotPetya ransomware attack that caused significant economic damage not just in Ukraine, but on a global scale. Attacks like these have fueled worries of cyberattacks with high magnitude and frequency once war were to break out. The 2022 cyber-operations conducted by Russia against Ukraine have thus far not matched those fears [MD22].

The gap has multiple potential explanations: For one, strategic withholding of information should not be discounted. With an ongoing war, operational discretion, censorship, and propaganda measures are common to gain strategic advantages over the respective enemy[24] [Rai00].
Therefore, it is reasonable to consider that not all cyberattacks launched at Ukraine (or NATO partners) have been disclosed. Nevertheless, NotPetya-like attacks impacting a considerable amount of people, particularly civilians, cannot reasonably be hidden; their absence is accordingly not (fully) explained by the "fog of war".

Another potential reason might be that cyberwar operations may simply not be as suitable in active warfare as might have been assumed. Within this context, their effectiveness and strategic value could be overestimated; while their conduction (setup time, activation, and the unfolding effects) could also be too slow to be suitable in active conflict [MD22].

Nevertheless, successful defensive measures should not be discarded. Russia's conventional forces' performance has fallen far behind expectations. That operational (conventional) weakness might correspond with underwhelming cyberwarfare capabilities e.g., due to organizational issues or lack of resources [Bat22, p. 34-36].

Additionally, the unexpected defensive strength of Ukraine's conventional forces may correspond with enhanced cyber-defensive performance. Among others, potential reasons for this encompass a resilient digital infrastructure, effective and far-reaching public-private cooperation, and thorough, years-long preparation by Ukrainian institutions. After all, Ukraine has been at war for 9 years now; large-scale incidents like NotPetya might have been a sufficient warning shot to trigger respective defensive enhancements (as they apparently did for its conventional forces) [Bat22, p. 40-44].

[24] This applies in more than one way: There may be direct military value in hiding information from the public and subsequently the opponent's reconnaissance. Furthermore, successful attacks might be seen as detrimental to morale domestically, and a potentially useful fact that can be used in the opponent's information operations.

4 Adversaries

Within the realm of cybercrime, there is a vast and heterogenous set of adversaries involved in attacks. For example, some actors might operate alone or in small groups in a rather non-professionalized manner for financial reasons or prestige. Others are much more advanced in resources or techniques, but still act as independent entities for profit. We refer to those as "Private Actors" (or Attackers). State-affiliated (or state-backed) Actors, on the other hand, are typically backed by nation-states and have both the resources and the expertise to launch highly sophisticated attacks. The level of integration and association to the government may vary.

Within the scope of this thesis, we predominantly focus on Advanced Persistent Threats (ATPs), which describes sophisticated adversaries in terms of expertise and resources. ATPs may use multiple attack vectors, adapt to the targets' defensive measures and act on a longer term with strategic objectives. This differentiates them from "simple" cybercriminal groups due to the much higher associated threat potential. The critical infrastructure context makes these types of adversaries a natural focal point for this thesis, as these adversaries have a higher threat potential and may differ in motivation [NIS].

We shall now explore both broad types of (mostly APT-) adversaries; some of which were previously mentioned through their involvement in landmark cybersecurity attacks (see Chapter 3.1). Afterwards, the methods and resources available to these adversaries are explored in detail.

4.1 State-affiliated Actors

State-affiliated adversaries pose a significant threat to the cybersecurity of private and public entities, and as such, to critical infrastructure as well. They often conduct espionage or infiltrate and target critical infrastructure sectors such as energy, transportation, and healthcare, aiming to disrupt operations and cause significant economic and social damage [PS14, p. 2-4].

One well-known example of a state-affiliated adversary is a group known as "Fancy Bear" (or APT28). This group has been linked to the Russian government via the Main Intelligence Directorate (GRU) and is known for its involvement in high-profile cyberattacks, including the 2015 hack of the German Bundestag, the 2016 DNC hack[1] [Sli20, p. 19] and the 2017 NotPetya ransomware attack that caused severe financial damages (see Chapter 3.1.2) [Thi16]. More recently, the group has also been accused of carrying out the 2020 hack of several e-mail boxes of members of the Norwegian parliament [Lyn20].
Seven alleged group / Russian intelligence and military members have been charged in the United

[1]The Democratic National Committee (DNC) is an organ of the Democratic Party, one of the two dominant parties in the United States.

States on multiple counts due to their alleged “persistent and sophisticated computer intrusions affecting U.S. persons, corporate entities, international organizations, and their respective employees located around the world, based on their strategic interest to the Russian government” [Uni18].

Another example is APT10, also known as “Stone Panda”; it is a state-affiliated Chinese hacking group that has been active since at least 2009 [PwC17, p. 5]. APT10 has been linked to espionage activities against a variety of targets, including government agencies, defense contractors, and organizations in the technology, healthcare, and finance fields.
One of APT10’s notable campaigns is “Operation Cloud Hopper”, a multi-year cyber espionage campaign targeting managed service providers (MSP) and their customers. The group used a variety of tactics, including spear-phishing emails, malware, and Social Engineering, to gain access to the MSPs’ networks and then move laterally to access their customers’ networks. The campaign resulted in the theft of sensitive intellectual property and other confidential data from a wide range of targets [Bar18; PwC17].
The group has been linked to the Chinese Ministry of State Security (MSS), an intelligence agency. The group is believed to be part of a larger Chinese cyber espionage apparatus that includes other state-affiliated hacking groups. [Bar18].

The inner workings of such state-affiliated actors are illusive and difficult to get an insight into. This is fueled by the necessary secrecy all such groups have to conduct to remain unexposed, and further hardened by active or passive government support. For one, the government association provides these groups with resources or finances as well as protection: their activities are illegal, but either the state chooses to look away, actively protects them or somewhat legalizes the activities by (loosely) integrating them into respective state agencies. Their advanced measures to remain unidentified (e.g., through anonymization techniques, aliases, and general operational security measures) also make the government connection difficult to trace, which is often in both parties’ interest [Vin17, p. 11].

Conti Leaks

Considering this, the 2022 “Conti Leaks” publication provides unusual insight into what such groups function like internally. Conti is a cybercrime group known for their use of ransomware attacks since at least 2019; the name is derived from the Conti ransomware the group distributes for many of its attacks. As other groups like “Trickbot”, they are suspected to be part of the larger Russian “Wizard Spider” cybercrime group, with their origins likely reaching back to 2018 under the name “Ryuk” [PRO22, p. 4].

The leak, published on the Twitter account @ContiLeaks days after the start of the Russian invasion of Ukraine in February 2022, contained over 168,000 messages as part of chat logs. They originated with Conti’s Jabber and Rocket.Chat servers and have been assessed as appearing authentic [GCB+23, p. 2]. In them, the group discusses several topics such as malware development or negotiations with ransomware victims; they provide insight into operations around recruitment processes, internal hierarchies, and finances through leaked Bitcoin addresses [GCB+23].

Based on the leaked chats and included Bitcoin addresses, researchers have inferred ransomware-related income of 104.4 million USD [GCB+23, p. 5] (including pre-2019 under the Ryuk brand). It appears to have moved significantly to a business model called “Ransomware as a Service” (RaaS). In some respects, the group operates quite business-like: It posted unsuspecting job offerings on

Russian forums and freelance websites, and ransomware advertisements as well as more illicit-looking job postings on forums and messengers such as Telegrams and Jabber. For example, they recruited spammers or bot herders (owners of botnets). Recruiting was backed by "HR specialists", although the legitimacy of its operations was frequently questioned by members[2]. In terms of structure, Conti is divided into smaller teams that appear to be headed by their organizational leaders; the actual power lies mostly with top five users [GCB+23, p. 7-9].

With the start of Russia's invasion of Ukraine in 2022, the group' leadership posted a pledge of "full support" to the Russian government only hours later. While most of its members were based in Russia, others were not - and not all members welcomed the close allegiance. This introduced destabilizing factors into the group's inner workings. Besides Conti Leaks, further disclosures - Trickbot Leaks - released materials on the inner workings of the group to the public. This included "doxing PDFs"[3] with compiled information of some members [Wri22, p. 3-5].
Although it is not clear exactly why (though likely a combination of pressure through leaks and inner dissent), the group appears to have disbanded in May 2022 [BK22].

4.2 Private Actors

While state-affiliated actors are arguably the higher-profile threat to critical infrastructure security, private actors should also be considered in this context. In contrast to the former, the latter is less motivated by (geo)-political contexts and not actively or passively protected by the government or supplied by it via financial means or other types of resources.

Instead, private actors typically operate with financial goals in mind; they achieve those through various criminal activities. They possess diverse skill sets and motivations associated with those activities. Some actors are highly sophisticated and operate as profit-driven cybercriminal organizations. They engage in illicit activities like ransomware attacks, data breaches, and financial fraud to exploit vulnerabilities in (critical infrastructure) systems for profit. Examples of such groups include the "REvil" ransomware group, responsible for high-profile attacks on organizations worldwide [BGAC14, p. 2-4].

Cybercriminal attacks on critical infrastructure have already been documented; a high-profile example is the 2021 Colonial Pipeline ransomware attack in the United States. A hacker group called "Dark Side" managed to hack and infect the pipeline operator's infrastructure with ransomware; subsequently, the pipeline was rendered inoperable on May 7, 2021. This immediately caused fears of a gasoline shortage and panic buying in the Southeastern U.S., which is the region the pipeline usually supplies. As President Biden declared a state of emergency, the company - under supervision of the FBI - already paid a ransom of 75 Bitcoin (which was around 4.4 million USD)[4].
DarkSide thereafter supplied a decryption tool, and operations were resumed on May 12, 2021.
While the disruption was ultimately short-term, this incident can be seen as an exemplary disruption of critical infrastructure (i.e., gasoline) motivated by cybercriminal, financial goals [EV21].

[2] At least by those recruited under a somewhat legally appearing pretext

[3] Doxing refers to the practice of revealing an online persona's real identity, e.g., via name and address, typically for malicious intent.

[4] The FBI later recovered most of the ransom

In terms of internal organization of such groups, there are different forms of structure; they can be classified by their respective Targets (online, offline, or both) and further categorized by their level of organization (more / less) [BGAC14, p. 4-7] [McG12, p. 4]:

Online **Swarms** Spontaneous operations solely online, possess a certain virality and connection through a shared purpose

Hubs Directed operations, with core groups of members that are linked to a wider net of associates

Hybrid **Clustered Hybrids** Small numbers, operations both on- and offline, narrow focus at specific methods, locations, activities

Extended Hybrids Lesser centralization level, tend to have a not as narrow focus as clustered hybrids

Offline **Aggregates** Similar to classic forms with a rather lose organizational form, such as classic street gangs, burglary groups

Hierarchies Strong hierarchical structure, comparable to "crime families" (e.g., mafia groups)

In addition to such cybercriminal organizations, there are also "hacktivist"[5] groups - also called collectives - that conduct cyberattacks as a means of promoting ideological or political agendas. It has been a long-standing concern that these groups potentially target critical infrastructure sectors to make a statement or raise awareness about specific issues, either targeting (typically large) companies or government institutions - something that has sometimes been referred to as a Cyber- or "Digital Pearl Harbor" [BS12].

Anonymous, a loosely associated international network of activists, is a well-known example of a hacktivist collective[6] that has conducted cyber-operations against various targets. It brands itself as anarchic hivemind of freedom fighters. The decentralized collective formed around 2003; they turned towards hacktivism in 2008 when they targeted the Church of Scientology with "Project Chanology" comprised of actions such as DDoS attacks or flooding their fax machines [Und09, p. 125-126].

In the early 2010s, Anonymous' popularity peaked due to their involvement in high-profile protest movements such as Occupy Wall Street[7] and its international offshoots, as well as the Arab Spring[8]. Other activities related to vigilantism, for example targeting websites that hosted child pornography [Col13].
In relation to critical infrastructure, the group has conducted hacks e.g., of United States law enforcement, which led to the release of over 200 GB of data including e-mails, internal intelligence, and reports ("BlueLeaks") [Gre20a].

[5] Hacktivist or hacktivism is a portmanteau comprised of hacking and activism
[6] By McGuire's typology above, Anonymous would be classified as a Swarm.
[7] A New York-based protest movement in 2011 against social and economic injustice, the influence of (financial) corporation in politics and lack of banking oversight
[8] A series of protest movements and revolutions in the Arab world, starting in Tunisia

Another example is “OpIsrael”, an annual coordinated cyberattack on various Israeli websites mostly related to the government and companies. In its first attack in 2013, hundreds of websites were disrupted, though the Collectives’ claim of resulting large-scale impact such as an alleged internet failure throughout Tel Aviv were false [Sha13]. While in the case of Anonymous, no critical services were disrupted, its various operations indicate that hacktivist collectives are a notable threat to cybersecurity and therefore should be considered in relation to critical infrastructure security [Kel12].

All in all, the rise of private actors in the cybercriminal space poses significant challenges for the security of critical infrastructure. Their activities can disrupt vital services, compromise sensitive data, and inflict financial losses on organizations. Moreover, private actors often take advantage of emerging technologies, such as ransomware-as-a-service (RaaS) platforms, making it easier for less technically skilled individuals to engage in cybercriminal activities.

4.3 Methods and Resources

In Chapter 3, we have introduced exemplary cyberattacks and discussed different types of adversaries associated with those (and many more), giving insights into the *What*, *Who*, and *Why* of cyberattacks on critical infrastructure.

In contrast, this section aims to shed light on the *How*, i.e., which methods and resources these adversaries employ or acquire to pursue their activities. To do so, we will explore the technical factor - the acquisition and application of cyberweapons, followed by Social Engineering as an exploitation technique of the human factor.

4.3.1 Cyberweapons

A potential source of resources for malicious actors are leaked cyberweapons, tools or Zero-day exploits. These may be intentionally or accidentally released or sold in auctions or more private settings - such as darknet platforms. Like many other illicit activities, auctions for exploits, malicious software or entire cyberwarfare-suits are often organized through darknet channels and the underlying funds exchanged via cryptocurrencies [GJLU23].

As Figure 4.1 indicates, this has become a vast illicit sector, with overall monetary exchanges through illicit addresses having surpassed the 20 billion USD mark in 2022[9]. Overall, this is a growing business - and the sale of such exploits, cyberweapons and related tools is arguably becoming an increasing issue for cybersecurity - accordingly, we will explore those in this section through the lens of Darknet Auctions.

[9]This encompasses various illicit activities, including circumvention of Russia-related sanctions or online scams - but it nonetheless underlines the vast size of the darknet ecosystem that also hosts these cyberwarfare-related activities

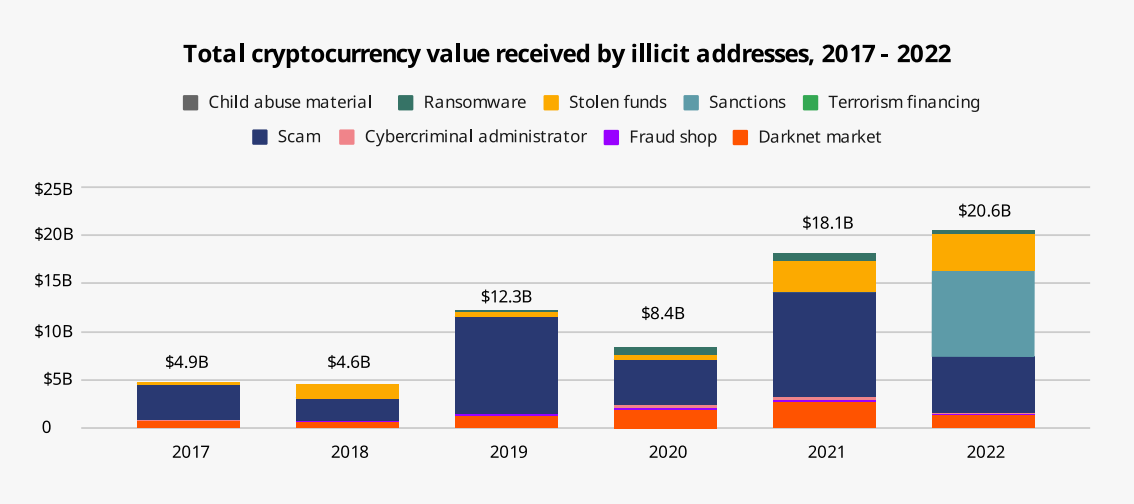


Figure 4.1: Development of total value of cryptocurrencies that were received through illicit addresses in the period 2017 to 2022. Image Source: [GJLU23, p. 5]

Darknet Auctions

A prominent example of (attempted) Darknet auctions of cyberweapons are the leaks published by a group called "The Shadow Brokers"[10]. We will therefore take a closer look on this occurrence as a representative of this class of resource acquisition.

In August 2016, a Twitter account with the handle @shadowbrokerss was created and started posting about a cyber weapons auction relating to the "Equation Group", multiple times, on August 13. The tweets[11] contained links to a Pastebin[12] containing a PGP signed message. In it, they claimed to have found cyberweapons made by the creators of Stuxnet, Duqu, and Flame ("Equation Group") by hacking them, thus gaining access to their source code repository.

As discussed in Chapter 3.1.1, Stuxnet is a worm that is understood to have been created as a cyberweapon in a collaboration between the United States and Israel for the purpose of sabotaging the Iranian nuclear program. The "Equation Group" had been heavily implicated in the malware's origin and is suspected of being tied to the United States' NSA. Both Duqu and Flame are closely related to Stuxnet and as such also linked to Equation Group (see Chapter 3.1.1). The Shadow Brokers group uploaded a set of "free files" to convince potential buyers of the hacking claim's veracity.

[10]The name is likely a reference to a character from the Mass Effect video game series, where the "Shadow Broker' is the powerful and elusive leader of a galaxy-wide organization dedicated to collecting and selling information.

[11]Since removed, the tweets are still accessible via the Wayback Machine under `https://web.archive.org/web/20160818115427/https://twitter.com/shadowbrokerss`

[12]The whole message is still available via the Wayback Machine under `https://web.archive.org/web/20160815172902/https://pastebin.com/JBc`

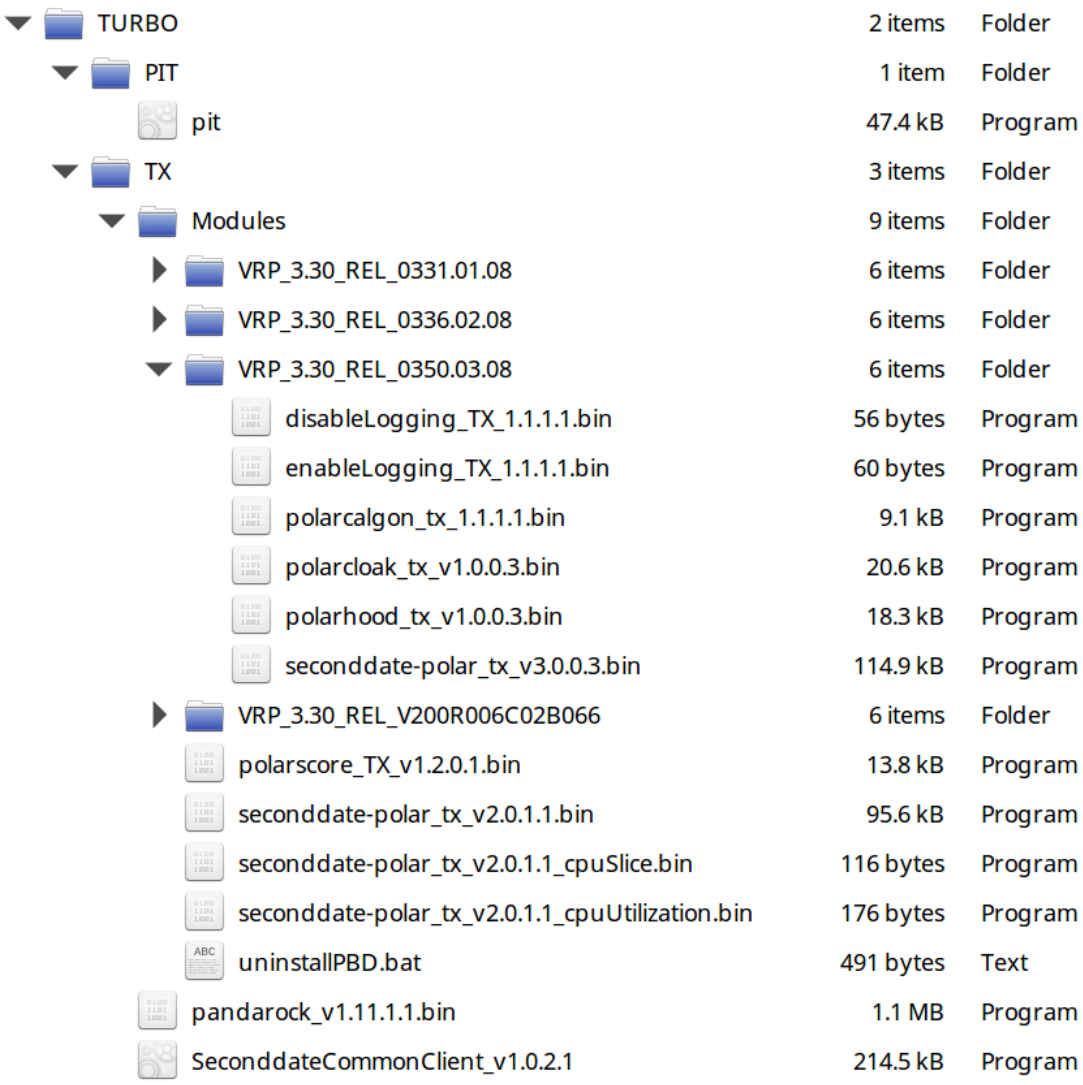


Figure 4.2: One of the pictures published by the "Shadow Brokers" group to as evidence of the "Equation Group" hack. Source: `https://imgur.com/a/sYpyn`

The Pastebin message also linked pictures cited as evidence of the claims' truthfulness. A sample image - displaying folder structures of the hack - can be seen in Figure 4.2. For interested people to gain access, they further announced an auction[13] with an unspecified end-date. The group did not disclose the actual contents of the auction package at the time.

However, this did not turn out to be the group's last publication on that matter: Multiple publications starting from October 2016 gave further insight into the inner workings of the "Equation Group" - including a list of allegedly hacked servers and further screenshots of folders structures relating to the group's claims of the hack.

[13]The auction was set up as a highest-bidder auction via a Bitcoin address - whoever sent the highest amount of Bitcoin to it was claimed to receive access to the files.

In April 2017, the group released the password to the encrypted files from the initial publication, suggesting the auction had not proved successful - thus revealing further exploits [Cox17b]. This had been preceded by the group "quitting", accompanied with some additional files [Cox17a].

One week later, this was followed by the "most damaging' release yet including several newly disclosed Windows exploits. Those contained vulnerabilities for multiple software products, including EternalBlue [Goo17] which had been used for Stuxnet[14]. Four Windows vulnerabilities[15] were patched one month ahead of the leak, suggesting Microsoft had likely been tipped off by Equation Group (or the NSA themselves) to prevent them from surfacing as unpatched Zero-day exploits. The NSA would have been able to identify these vulnerabilities as likely to be released back in January 2017, based on screenshots relating to another auction [Goo17].

Nonetheless, there is no evidence for the theory and alternative explanations are feasible as well: For example, Microsoft could have purchased the information from the Shadow Brokers themselves (or have received the information by a third-party). Another hypothesis revolved around an incidental finding and patching by Microsoft, with the Shadow Brokers group realizing their (formerly Zero-day) exploits had ceased functioning due to the March 2017 updates. In consequence, the Shadow Brokers would then have released the exploits for publicity reasons. This would not explain the timing of patches and Shadow Brokers release, as in that case, a leak immediately after Microsoft's patches would have had a much larger and disruptive impact due to more devices remaining unpatched at the time of disclosure. In sum, the most likely explanation remains a tip from the Equation Group / the NSA [Goo17].

4.3.2 Social Engineering

Social Engineering refers to the use of psychological manipulation techniques to deceive individual people or groups into divulging sensitive information or performing actions detrimental to their own interests and responsibilities. Social Engineering attacks involve the exploitation of human behavior and tendencies, such as trust or fear [WZS21, p. 1].
They are typically branched into two types of attacks - Human or Computer-based attacks. However, a three-pronged classification into Technical, Social and Physical-based schemes is also possible; the latter pays respect to *how* the attack is executed rather than by *whom* [SK19, p. 3].

In cybersecurity, Social Engineering attacks are a significant threat because they often target the human element of an organization, which can be the weakest link. For example, an attacker might use a phishing email to trick an employee into clicking on a malicious link or downloading an infected attachment by posing as their superior, thereby gaining access to sensitive information or systems. Attackers may constantly adapt and change their methodology, making defensive preparations difficult.
For example, the *Enkeltrick* (grandchildren trick) is a common method in Germany with perpetrators convincing elderly victims of being their (grand-) children in immediate need of larger sums of money, typically to prevent catastrophic consequences.

[14] Which again reiterated the link between Stuxnet and Eternal Group
[15] EternalBlue, EternalRomance, EternalChampion and EternalSynergy

Social Engineering attacks can also target employees with privileged access, such as system administrators or network engineers. In such cases, an attacker might use a pretexting technique, where they impersonate a trusted authority or person to convince the employee to disclose login credentials or perform actions that give the attacker access to critical systems.
In recent years, such pretexting attacks have become increasingly more frequent, with attackers posing as an authority figure in a fictional scenario that puts the victims under (emotional) pressure to act.

In fact, many such schemes rely on a four-phase process [SK19, p. 2]:

1. Research and information gathering: Initially, victims are selected by the attacker by their desired criteria.
2. Relationship Initiation: The attacker proceeds with the attack and establishes contact with the victim in order to build trust.
3. Execution: The attacker further (emotionally) manipulates the victim, requesting and pushing them towards the desired action.
4. Exit: Once the attacker reaches their goal (or decides to abort), they exit the relationship leaving as little proof as possible.

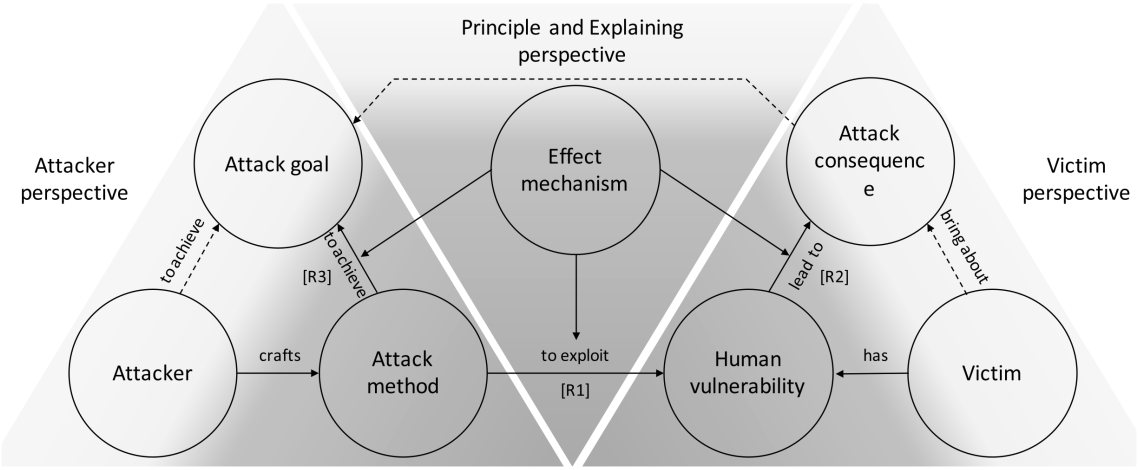


Figure 4.3: Conceptual model describing how Social Engineering attacks work; Model and image source: [WZS21]

Underlying Mechanisms

We shall now take a closer look at how Social Engineering attacks work from different perspectives. As modeled by Wang et al., Figure 4.3 models the relationship from both the attacker's and victim's perspective as well as an explanatory perspective. The attacker (left side) crafts an attack method to achieve their attack goal, thereby exploiting human vulnerability of the victim. The victim (right side) has the vulnerability that brings about the attack consequence (e.g., loss of financial means). From an explanatory perspective (middle), there are various effect mechanisms that explain how

attack methods achieve the goals and how attack methods exploit human vulnerability through different aspects, as well as why these vulnerabilities lead to the attack consequences [WZS21, p. 2].

These aspects and their associated effect mechanisms can be categorized as follows [WZS21, p. 2-10]:

- Persuasion
- Social Influence
- Cognition, Attitude and Behavior
- Language, Thought and Decision
- Emotion and Decision-Making

Effect Mechanisms

We will now take a closer look at a subset of those effect mechanisms and how they may apply to cybersecurity scenarios.

The perceived level of similarity influences the victim's opinion of the attacker, which further impacts the likeliness of them "helping" the attacker. (Moderate) distraction may also reduce resistance by disrupting the process of counter-argumentation (time pressure and thought overloading also have a similar impact as a sort of Human DDoS attack [WZS21, p. 6]). Furthermore, the perception of an authority figure or otherwise qualifying credibility tends to increase compliance [WZS21, p. 3].

Persuasion may also be modeled through two routes - central and peripheral [MN16]. The central route occurs when the target is motivated through factors and able to think about the issue in question. The motivation is provided e.g., through personal importance or interest. If the presented arguments are strong, the target is likely to be convinced; but not if they are weak. The peripheral route, on the other hand, may occur if the target is not able to think clearly, e.g., when being distracted. As the arguments are not thoroughly processed, automatic acceptance may be triggered by familiar, easy-to-process statements, and quantity of arguments increases likelihood of acceptance [WZS21, p. 3-4]

This model can be applied to our cybersecurity context, as IT specialists (e.g., administrators, cybersecurity officers) are highly involved and therefore attacks on them require a sophisticated level of (strong) argumentation. On the other hand, lowly involved personnel (such as security guards or facility managers) typically lacks the technical insight or other motivational factors and thus can be targeted through peripheral cues. Of course, both routes of persuasion are non-exclusive and may well occur at the same time [WZS21, p. 4].

There are also various effect mechanisms in the aspect of social influence through social norms, morals, and expectations. These may induce behavioral changes e.g., through group influence and conformity with varying effects depending on group size and cohesion. These can be tied into social exchange theory, which considers "social goods", such as information, services, and affection, in a way comparable to material goods [CCRN13]. Accordingly, actions like helping and displaying kindness are normally associated with reciprocity - to return the favor.

This, too, can be used in (reverse) Social Engineering attacks initiated by an orchestrated favor (e.g., by impersonating IT service) which, upon execution, is then followed by another request (e.g., requesting a password). Other approaches may be based on exploiting morality and social responsibilities of targets, or other reciprocity-based methods such as self-disclosure (disclosing personal information to induce emotional connection and disclosures in return) [WZS21, p. 5].
Of course, there are many more effect mechanisms that can be applied in Social Engineering attacks, such as framing, use of specific language to evoke thought, or emotional manipulation to influence decision making [WZS21, p. 7-8].

Human Vulnerabilities

Through various effect mechanisms, Social Engineering attacks exploit many different psychological vulnerabilities in humans. While a deeper analysis of those is outside the scope of this thesis, they can be roughly summarized as follows [WZS21, p. 9-10]:

Cognition and Knowledge Vulnerabilities arising through factors such as inexperience, ignorance, prejudices, thought heuristics or simply lack of knowledge.

Behavior and Habit Humans tend to (sub-consciously) establish fixed action patterns, i.e., repetitive and periodical behavior, which can subsequently be exploited (e.g., repeated use of a certain website by an employee opens up attack scenarios via manipulation of said website).

Emotion and Feeling Strong emotions such as anxiety, fear or excitement can significantly lower cognitive abilities, e.g., by evoking guilt to induce desired action.

Human Nature A complex and wide set of vulnerabilities arising from personality traits (e.g., neurotic individuals may be easier targeted through induction of fear), human nature (e.g., exploiting compassion by emulating being in need of help by the target), or simply individual positive or negative characteristics (positive e.g., kindness, negative e.g., envy).

5 Countermeasures

In the previous chapters, we have defined critical infrastructure, analyzed known cyberattacks as well as their perpetrators, and lastly, we have looked at origins of resources and methods often used to conduct such attacks. To prevent or mitigate future attacks, organizations can apply various kinds of countermeasures.

In this chapter, we will look at frameworks as a structured roadmap to analyzing and improving cybersecurity, technical interventions such as IDPS, approaches to combat Social Engineering techniques, and avenues for legislative intervention to further standardize and enhance cybersecurity.

5.1 Social Engineering Defenses

The size, diversity, and flexibility of Social Engineering attacks makes preparation and defense inherently difficult. In our context, the arising vulnerabilities are aplenty and reach far beyond mere pretexting. Attackers may be able to gain physical access to separated networks by using security lapses or passing it through socially engineered attacks. While classical audits may be able to systematically reduce weaknesses in protocols or security infrastructure, the human factor is difficult to be addressed in a generalized and reliable manner (see Chapter 4.3.2).

One of the reasons for this is the adaptability of attacks: While employee training might help them to gain general knowledge and awareness of the issues, they cannot cover all possibilities. While cybersecurity training may deal with phishing emails as they currently appear, attackers may simply change the scenario [Wol22, p. 291]. For example, e-mails with the attacker posing as the supervisor may simply switch the underlying pretext once their current iteration loses its efficacy.

Overall, research provides several avenues of countermeasures, which can and should be combined into a holistic approach. This is often implemented as a Depth in Defense structure, which consists of multiple levels of defenses as a mixture of different measures [CS16, p. 34-35]:

- Security Policy
- Education and Training
- Network Guidance
- Audits and Compliance
- Technical Procedures
- Physical Guidance

Educational seminars may have their use-cases and benefits but are not considered a stand-alone solution to address Social Engineering [SBP17, p.14]. Some researchers, such as Angela M. Sasse, even suggest that some trainings can have a harmful effect if they include a perceived breach of trust. Such lasting disruptions may for example occur, if ahead of an anti-phishing seminar, the leader conducted phishing attacks on employees on behalf of the employer [Wol22, p. 291].
Hence, trainings need to teach awareness and generalized skills to recognize such attacks in broader context, without antagonizing the end-users.

Some countermeasures take a technological approach, for example via the use of multi-factor authentication (MFA) systems. These systems require users to provide multiple forms of identification, often a password and a one-time code (through an authenticator app, SMS, or e-mail) to gain access. While this certainly can help in certain circumstances such as phished login credentials, in other cases - especially when the target has already been convinced to disclose sensitive information - this merely adds one more step.

Security policy, in general, should be well written and consider technical and non-technical safeguards [CS16, p. 34]. Furthermore, security measures should be appropriately complex and consider the workload they put on the end-users supposed to uphold them. For example, many password policies require frequent password changes or cryptographic complexity through using many different characters (e.g., mandating special characters, up- and lowercase, digits, etc.). This may not just take time away from productive work, but lead users to be antagonized and seek out short-cuts to make unusable policy usable. Therefore, good security policy needs to consider which level of complexity is appropriate in different circumstances to ensure usability [IS10].

Another example of security measures with unintentional counterproductive effects is the over-usage of warnings. This may occur with dialog boxes when opening certain files or performing actions in routine settings. If users must confirm these warnings *all the time*, most of them tend to ignore warnings altogether because of frequent false positives [KMS12, p. 6-7]. As a result, Krol et. al propose re-sensitizing users by only showing warnings, iff there is both:

1. Genuine concern of significant danger
2. No certainty of maliciousness

In other cases, the action should either be blocked right away (1., but not 2.) or no warning is required (Not 1., but 2.) [KMS12, p. 7].

An example for adherence to this principle are “smart” MFA systems. For example, Amazon does not always require confirmation of orders or logins. Instead, purchases or logins that seem out of the ordinary - e.g., using an abroad IP address, unknown devices, or entirely atypical purchases - may trigger the additional layer of security in these cases of doubt. Thereby, the user is only further involved if the system thinks it is required [Wol22, p. 292-293].

5.2 Structured Frameworks

Frameworks are a valuable tool for improving cybersecurity by providing organizations with a structured and systematic approach to manage and mitigate cyber-risks. By offering a comprehensive set of guidelines, best practices, and controls, such frameworks provide a path for establishing effective cybersecurity programs.

A prime example and representative of these frameworks is the NIST Cybersecurity Framework, which we will take a closer look on in this section. As part of that, we will delve into its components, exploring how it can enhance an organization's cyber-resilience and enable appropriate, proactive risk management.

5.2.1 NIST Cybersecurity Framework

The NIST Framework for Improving Critical Infrastructure Cybersecurity is a comprehensive guideline developed by NIST. It builds upon the institution's previous work and was first published in 2014, after the U.S. Cybersecurity Enhancement Act of 2014 widened NIST's role to include development of such frameworks; its current version 1.1 was released in 2018. This framework provides organizations with a structured approach to managing and mitigating cybersecurity risks associated with critical infrastructure. It thus serves as a tool for enhancing cybersecurity practices, promoting risk-based decision making, and fostering collaboration between relevant public and private sector entities [Nat18, p. v - vi].

The NIST Framework consists of three main components: The Core, Framework Implementation Tiers, and Framework Profiles. The Core presents a set of cybersecurity activities, outcomes, and informative references that organizations can tailor to their specific needs. It provides a flexible and customizable foundation for building robust cybersecurity programs [Nat18, p. 3]. Figure 5.1 illustrates the Framework Core's structure, which may be described as follows [Nat18, p. 6 - 8]:

- Functions: These high-level cybersecurity activities, Identify, Protect, Detect, Respond, and Recover, guide organizations in achieving effective cybersecurity by "organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities" [Nat18, p. 6].
- Categories: The Functions are broken down into groups called Categories, associated with programmatic needs as well as particular activities (e.g., Asset Management).
- Subcategories: Within each Category, Subcategories provide detailed and actionable (non-exhaustive) cybersecurity tasks or actions (technical and management) that organizations can undertake to address risks and challenges.
- Informative References: These references point to sources such as standards, guidelines, and best practices, offering additional guidance to support organizations in implementing the Framework effectively.

Figure 5.1: Structure of the Framework Core. Image enhanced via Icons8 Upscaler; original image source: [Nat18, p. 6]

The Implementation Tiers offer a framework for organizations to evaluate their cybersecurity maturity level and ability to handle cybersecurity risks effectively. By assessment of their current tier and identification of desired targets, organizations can establish a roadmap for improving their overall cybersecurity. Via progressing through the tiers, organizations can enhance their cybersecurity practices and risk mitigation depending on favorable cost-benefit analysis, thereby improving their protection. The tiers are described as follows [Nat18, p. 9-11]:

1. Partial: Organizations have limited cybersecurity awareness and ad-hoc practices. They may lack a formal cybersecurity program, relying on reactive measures instead of proactive risk management. Cybersecurity activities are inconsistent, and there is a limited understanding of potential threats and vulnerabilities.
2. Risk Informed: Organizations in this tier demonstrate an improved understanding of cybersecurity risks. They have started the development of risk management processes and implement controls based on their identified risks. However, the practices may not be consistently applied throughout the entire organization, leaving room for potential gaps in cybersecurity defenses.
3. Repeatable: Organizations have formalized cybersecurity programs and processes, with established policies, procedures, and standards guiding their cybersecurity practices. Cybersecurity controls are implemented consistently; they actively monitor their systems and respond to incidents. Nonetheless, there may still be room for improvement in terms of adapting to evolving threats and fully integrating cybersecurity into the business processes.

4. Adaptive: Organizations have proactive and constantly evolving cybersecurity approaches. They continuously improve their capabilities based on lessons learned, threat intelligence, and the industry's best practices. These organizations have a comprehensive understanding of their cybersecurity risks and effectively manage them. They are both rapid and agile in responding to emerging threats and have a culture of cybersecurity throughout the organization.

Lastly, Profiles enable organizations to align their cybersecurity objectives with their business requirements, risk tolerance, and the resources available to them. While the Current Profile denotes the currently achieved outcomes, the Target Profile points to the outcomes required for achieving the desired cybersecurity goals; the gap between them thereby indicates potential gaps that should be addressed via an action plan in order to meet the objectives [Nat18, p. v - vi, 4, 11].

One of the NIST Framework's strengths is its adaptability. It is designed to accommodate various industries, organizations of assorted sizes, and all levels of cybersecurity maturity. This flexibility allows organizations to adapt the framework to their specific context while still adhering to recognized best practices. The NIST Framework has gained widespread adoption and recognition both in the United States and internationally. For example, many organizations in Japan or the United Kingdom have embraced the framework, and more indirectly, the European Union's more recent cybersecurity legislation has in principle adopted the Core in the NIS Directive [SRH15, p. 21].

Due to its success, NIST is planning to update the framework within the near future [Kel23]. Its flexible nature, emphasis on risk management, and widespread adoption have made it a valuable resource for many organizations seeking to enhance their cybersecurity posture. By leveraging the framework's core principles, implementation tiers, and profiles, organizations can establish a proactive cybersecurity approach and build resilience against evolving cyber-threats, both in critical and non-critical infrastructure entities.

5.3 Intrusion Detection and Prevention Systems

An example for technical countermeasures[1] is the usage of IDPS[2], which we will briefly discuss as a representative for technical interventions. These systems can help identify and block suspicious network traffic that may be associated with intrusion into systems; that makes them a potential component in prevention and mitigation of cyberattacks.

These systems employ various techniques to identify and respond to potential threats, which includes intrusion attempts, malware infections, and anomalous network behavior. By analyzing network traffic, monitoring system logs, and employing signature-based or behavior-based detection methods, IDPS can provide real-time threat intelligence and take appropriate actions (i.e., alert responsible personnel or disrupt attack itself) [SM+07, p. ES 1, 2–2].

[1] There are many more - for example, "smart" MFA systems like Amazon's mentioned in Chapter 5.1 can be counted into this category as well.

[2] IDPS - also referred to as Intrusion Prevention Systems (IPS) - can be thought of as an extension to Intrusion Detection Systems (IDS), where the former adds preventive functionality to the latter's analytical detection function.

A strength of IDPS is their ability to provide proactive defense against a wide range of cyber threats. They can detect and block malicious activities at various stages, preventing or freezing breaches before they can cause significant harm. IDPS can also provide insights into the nature of attacks, aiding in incident response as well as (post-incident) forensic investigations [SM+07, p. 2-1 - 2-2].

However, IDPS can also be susceptible to false positives, where legitimate activities are flagged as malicious, leading to disruptions and unnecessary alerts. Weighing the desire for maximal detection and minimal false alerts is thus a key challenge. Moreover, IDPS may introduce network latency in high load scenarios (a serious drawback e.g., in use-cases requiring real-time activities) [SM+07, p. 4-12]. They might also require continuous updates to keep up with emerging threats, introducing an additional maintenance burden.
Recent advances in Machine Learning and Artificial Intelligence techniques may also be beneficial for improving detection rates and are currently a focus in research and development [HSU19].

All in all, technology-based interventions can be considered as an option for improving cybersecurity in vulnerable organizations.

5.4 Legislative Interventions

Interventions via laws and regulations constitute another possible path for enhancing cybersecurity within critical infrastructure. Whereas the measures introduced previously focused on providing organizations with the tools needed to enhance their defenses, laws and regulations provide the external (and mandatory) motivation to do so.

In Chapter 2.3 we already explored what the legislative foundation surrounding critical infrastructure looks like through respective regulations of the European Union up to the NIS Directive. The everchanging conditions - e.g., the rapid progress of information technology or developments within the pool of potential adversaries - imply a need for updating respective legislation as well.

We will therefore take an additional look at current developments within the regulatory space, through the NIS Directive's overhaul: The NIS2 Directive, which has been passed in December 2022 and is currently in the implementation phase by member states. Of course, this EU-centric perspective to a global problem is non-exhaustive: Specific challenges and environmental circumstances may differ in other jurisdictions - subsequently, other legislative measures may be indicated.

5.4.1 NIS2

The NIS2 Directive was the result of a process initiated by the European Commission to overhaul and adjust the NIS Directive that had been passed in 2016. While the Commission itself acknowledged significant cyber-resilience progress, a review of the directive determined weaknesses: The member states' large degree of freedom at defining and imposing cybersecurity requirements (and security- as well as incident reporting requirements) upon "economically significant" organizations led to a large variance ("fragmentation") among national implementations [Eur22a, Pmbl.].

This fragmentation can also be observed through the number of Operators of Essential Services (OES) in each member state. Figure 5.2 illustrates the results: While, for example, Estonia identified 10 such OES per 100,000 inhabitants, many other countries such as Germany, France or Spain identified well under a tenth that amount.

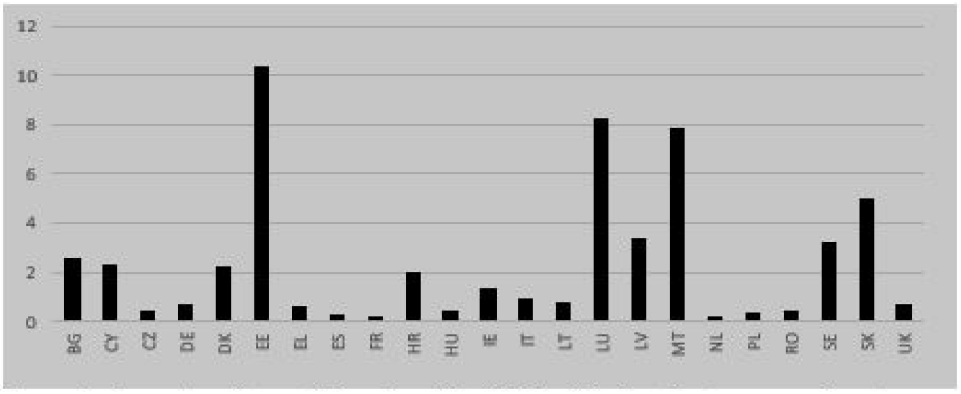


Figure 5.2: Number of Operators of Essential Services per 100,000 inhabitants, by member states. Image Source: European Commission via [Eur23b, p. 5]

This was seen as detrimental to the internal market, to cyber-resilience and respective cross-border service provisioning. The Commission's evaluation further found that NIS had been too narrow in terms of sector coverage; the rapid digitization (in part due to the COVID-19 pandemic) and further increased interconnectedness in the single market widening the appropriate scope for NIS2. Furthermore, ineffectiveness at supervision and enforcement of NIS' provisions as well as (still) lacking information sharing between member states were observed [Eur23b, p. 6].

NIS2 accordingly went into force replacing NIS in January 2023, although its provisions are in the process of being nationally implemented and must be phased in by October 2024 [Eur22a, Pmbl.]. Overall, its key changes revolve around three stated general objectives [Eur23b, p. 7-8] [Eur22a]:

- Increasing the level of cyber-resilience: Expansion of NIS' scope to include sectors such as public administration and social media, and to apply to medium and large-sized entities within relevant sectors. The member states' ability to adjust security rules was reduced to reduce regulatory fragmentation.
- Reduction of inconsistencies: Further alignment of rules for incident reporting, national supervision and enforcement as well as the responsible authorities' capabilities, and the overall scope of the directive (i.e., the logic behind whom the rules apply to or not).
- Improved cooperation and coordination: Increased trust and information sharing between authorities, rules and planning for response to large-scale incidents. For that purpose, the "European cyber crisis liaison organisation network'' (EU-CyCLONe) was established as a cooperation network for the national authorities responsible for cyber crisis management.

Overall, NIS2 can be seen as an indicated update to NIS, addressing shortcomings associated with NIS (also see Chapter 2.3.2). However, as national implementation into legislation is an ongoing process continuing well into 2024, the effectiveness of NIS2 cannot yet be determined, especially in those areas, where NIS was considered to not have succeeded [Van23, p. 31-32].

It does, however, demonstrate the still-ongoing evolution of essential infrastructure; with the threat landscape being able to shift quickly (e.g., Russia's invasion of Ukraine), the infrastructure itself changing (e.g., rapid digitization in part fueled by COVID-19's challenges), and the scope of what should qualify as critical always changing as well (e.g., growing dependence on the IoT supply chain) [Van23, p. 31-32]. These changes and challenges are clearly not limited to the European Union, therefore, constant adaptation through legal means is going to be an ongoing factor in many jurisdictions around the world for the foreseeable future.

6 Conclusion and Outlook

In summary, this thesis gave an overview over critical infrastructure, how it has been and could be attacked digitally, and which countermeasures can be taken against that. First, critical infrastructure was introduced, its historical development and evolution into its modern form described. This was put into a legal perspective by exploration of the corresponding regulations of the European Union.

Then, we investigated two major exemplary cyberattacks that affected critical infrastructure: First, Stuxnet was introduced as a landmark malware incident that ushered in the era of state-affiliated hackers developing and deploying cyberweapons in critical infrastructure of another country. Its sophistication and underlying resources (e.g., multiple Zero-day exploits) as well as novel target - the Iranian nuclear program - ensured its ongoing legacy in the cybersecurity space. Furthermore, NotPetya was explored as a 2017 ransomware attack onto Ukraine that affected multiple sectors qualifying as critical infrastructure; its likely deployment by Russia and usage of leaked exploits made it another prime example of such attacks. This was complemented with a look at cyberwarfare measures in the ongoing invasion of Ukraine by Russia.
Following that, an overview over the perpetrators - state-affiliated and private actors - was given in order to better understand their capabilities and motives.

Afterwards, we explored the methods and resources available to these adversaries: Exploits, tools and entire cyberweapon-suites can be leaked, illegally sold, and purchased, or sold via Darknet channels. The latter was investigated through the case of The Shadow Brokers, a group which attempted to auction hacked cyberweapons and later released them to the public.
In addition to that, Social Engineering was introduced as a psychological manipulation technique - an exploit of the "human factor". To explain the stunning success of these many-faceted attacks, we explored the underlying mechanisms and human vulnerabilities involved in it.

The gained insight was subsequently transformed into a non-exhaustive presentation of potential countermeasures. Accordingly, defensive measures against socially engineered attacks were introduced, followed by cybersecurity frameworks. As a widely adopted representative of its class, the NIST Cybersecurity Framework was examined as a possible roadmap for many organizations to analyze and improve their cybersecurity measures.
This was accompanied by the introduction of IDPS as a potential technical intervention to prevent and/or mitigate attacks. Finally, (further) legislative interventions - again focused on the European Union - were mentioned as a way of improving (digital) critical infrastructure security through regulatory means.

Ultimately - and circling back to the initial questions raised - this thesis finds that the cyberwar is already reality and cyberattacks on critical infrastructure have already become an increasingly serious issue. When looking at the EU's regulatory measures specifically, it is apparent that the response is late: While Stuxnet's warning shot already occurred in 2009-2010, it was only in 2013 that the Cybersecurity Strategy commenced a major shift towards horizontal legislation that arrived

with the Network and Information Security Directive (NIS Directive) in 2016. Further legislation built upon that foundation, and currently its successor, the NIS2 Directive, is in its implementation phase by the member states. Whether it has managed to solve the long-standing issues thus remains to be seen.

The vast and diverse set of adversaries, in this context most of them state-affiliated, is a looming and arguably growing threat for disruptions of our critical infrastructure. Especially Russia has demonstrated interest and knowledge in targeting countries both with information and cyberwar-operations; the latter has been e.g., demonstrated via NotPetya in 2017 and has been an ongoing factor in its invasion of Ukraine since 2022. The fact that we have *not yet* seen massive cyberattacks in this war should not be mistaken as an indication that we never will. Especially on a longer timeframe, the risk of such large-scale attacks is arguably high, and especially so in the current global security landscape.

At the same time, exploits, leaked cyberweapons and other resources created by intelligence agencies[1] are a risk; the hacking or leaking of such tools has become a factor in supplying adversaries with the resources they may use to provoke large-scale disruptions of critical infrastructure systems. The practice of collecting Zero-day exploits or accumulating cyberweapons by the state is criticizable, and from the defensive, cybersecurity viewpoint: At best counterproductive.

While the methods and supply chains of these adversaries are (more or less) known, acting on them is not an easy task. For the illicit use of Darknet and cryptocurrency channels, it is difficult to intervene legislatively without the danger of disproportionately encroaching upon personal freedoms of the many. Other avenues, such as adapting cybersecurity measures through acclaimed frameworks like NIST's, are generally promising. At the same time, an increased focus on defending against socially engineered attacks is highly indicated.

In fact, this thesis finds that there is no one easy solution applicable to all. Instead, a holistic combination of multiple approaches is much more promising. For example, using a framework to establish and evolve a (defense-in-depth) cybersecurity foundation is well supported by considerations of what the actual workflows and end-user contact should look like. Without an understanding of *why* certain processes should be performed the way they were specified, adherence is much less likely - on all paygrade levels. For example, this does not just apply to the unfortunate end-user opening a suspicious e-mail attachment; but it also applies to IT staff that may not always see the benefit in established security practices and subsequently seeks shortcuts (e.g., delaying patch days or circumventing authorization practices).

This can not only improve individual compliance but also reduces an organization's vulnerability for socially engineered attacks, which might otherwise be able to circumvent generally well-thought-out defensive measures. Adding technical solutions like IDPS may assist in stopping, detecting, or mitigating attacks where they occur. The government(s), on the other hand, can and should further assist these cybersecurity transitions by providing the regulatory framework to support and demand reasonable measures. At the same time, it is apparent that more research in this field is not only warranted but needed.

[1] Or affiliated, sponsored or otherwise connected groups

This thesis should accordingly be understood as a plea for making cybersecurity in these critical environments a goal that is present in all relevant stages of business development and processes, actively involving all stakeholders. More than that, it is a call for a transition to a more holistic view on these topics - in order to invoke innovative solutions able to protect our modern critical infrastructure.

While there has certainly been progress on many fronts, a much higher awareness of the underlying problem(s), the potentially deadly consequences, and the already-available ways of protection is needed throughout society. The current state of the art should therefore be understood as only the beginning - and a foundation to start from as we move towards a secured critical infrastructure and society of the future.

Bibliography

[ABKY93] Å. E. Andersson, D. F. Batten, K. Kobayashi, K. Yoshikawa. "Logistical Dynamics, Creativity and Infrastructure". In: *The Cosmo-Creative Society*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993, pp. 1–16. ISBN: 978-3-642-78460-6. DOI: 10.1007/978-3-642-78460-6_1 (cit. on p. 15).

[ABW10] D. Albright, P. Brannan, C. Walrond. *Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant?* 2010. URL: https://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf (cit. on pp. 36, 37).

[Ass09] M. Assante. "Infrastructure Protection in the Ancient World". In: *2009 42nd Hawaii International Conference on System Sciences*. 2009, pp. 1–10. DOI: 10.1109/HICSS.2009.260 (cit. on pp. 14, 15).

[Ban19] A. Bannister. *When the screens went black: How NotPetya taught Maersk to rely on resilience – not luck – to mitigate future cyber-attacks*. Updated version dated July 6, 2021. Dec. 2019. URL: https://portswigger.net/daily-swig/when-the-screens-went-black-how-notpetya-taught-maersk-to-rely-on-resilience-not-luck-to-mitigate-future-cyber-attacks (cit. on p. 43).

[Bar18] B. Barrett. *How China's Elite Hackers Stole the World's Most Valuable Secrets*. Dec. 2018. URL: https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/ (cit. on p. 48).

[Bat22] J. Bateman. "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications". In: (Dec. 2022). URL: https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657 (cit. on p. 45).

[BBB+23] M. Beyer, V. Blateau, F. Bitzer, F. Dietrich, C. Lammerskitten, B. Lück, R. Richter, C. Rudolph, T. Vogel. *Der Digitale Knoten Stuttgart wird Realität*. Jan. 2023. URL: https://digitale-schiene-deutschland.de/Downloads/202301%20Der%20Eisenbahningenieur%20DKS-Sachstand.pdf (cit. on p. 17).

[BCFD16] R. Bayindir, I. Colak, G. Fulli, K. Demirtas. "Smart grid technologies and applications". In: *Renewable and Sustainable Energy Reviews* 66 (2016), pp. 499–516. ISSN: 1364-0321. DOI: https://doi.org/10.1016/j.rser.2016.08.002 (cit. on p. 16).

[BGAC14] R. Broadhurst, P. Grabosky, M. Alazab, S. Chon. "Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime". English. In: *International Journal of Cyber Criminology* 8.1 (2014), pp. 1–20. ISSN: 0974-2891 (cit. on pp. 49, 50).

[BK22] Y. Bogusalvskiy, V. Kremez. *DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape*. Available via the Internet Archive. May 2022. URL: https://web.archive.org/web/20220601075352/https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape (cit. on p. 49).

[Bor17] C. Borys. *The day a mysterious cyber-attack crippled Ukraine*. July 2017. URL: https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine (cit. on p. 42).

[BPBF11] B. Bencsáth, G. Pék, L. Buttyán, M. Félegyházi. "Duqu: A Stuxnet-like malware found in the wild". In: *CrySyS Lab Technical Report* 14 (Oct. 2011). v0.93, pp. 1–60. URL: https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf (cit. on p. 39).

[BPBF12] B. Bencsáth, G. Pék, L. Buttyán, M. Félegyházi. "The Cousins of Stuxnet: Duqu, Flame, and Gauss". In: *Future Internet* 4.4 (2012), pp. 971–1003. ISSN: 1999-5903. DOI: 10.3390/fi4040971 (cit. on p. 39).

[BS12] E. Bumiller, T. Shanker. *Panetta Warns of Dire Threat of Cyberattack on U.S.* Oct. 2012. URL: https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html (cit. on p. 50).

[Bun16] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Das IT-Sicherheitsgesetz - Kritische Infrastrukturen schützen*. Feb. 2016. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf (cit. on p. 26).

[Bun21a] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Kritische Infrastrukturen - Sektoren- und Brancheneinteilung*. July 2021. URL: https://www.bbk.bund.de/SharedDocs/Downloads/DE/KRITIS/kritis-sektoren-brancheneinteilung.pdf?__blob=publicationFile&v=3 (cit. on p. 13).

[Bun21b] Bundesrepublik Deutschland. *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)*. June 2021. URL: https://www.gesetze-im-internet.de/bsig_2009/__2.html (cit. on p. 13).

[Bun22] Bundesamt für Sicherheit in der Informationstechnik (BSI). *BSI - NIS Directive*. Dec. 2022. URL: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/NIS-Richtlinie/nis-richtlinie_node.html (cit. on pp. 26, 27).

[CB17] H. Carrapico, A. Barrinha. "The EU as a Coherent (Cyber)Security Actor?" In: *JCMS: Journal of Common Market Studies* 55.6 (2017), pp. 1254–1272. DOI: https://doi.org/10.1111/jcms.12575 (cit. on pp. 24, 25).

[CCRN13] K. S. Cook, C. Cheshire, E. R. W. Rice, S. Nakagawa. "Social Exchange Theory". In: *Handbook of Social Psychology*. Ed. by J. DeLamater, A. Ward. Dordrecht: Springer Netherlands, 2013, pp. 61–88. ISBN: 978-94-007-6772-0. DOI: 10.1007/978-94-007-6772-0_3 (cit. on p. 56).

[Cli98] B. Clinton. *PDD-63 - Critical Infrastructure Protection, 5/20/1998*. May 1998. URL: https://clinton.presidentiallibraries.us/items/show/12762 (cit. on p. 18).

[Col13] G. Coleman. “Anonymous in context: The politics and power behind the mask”. In: (Sept. 2013). URL: https://www.cigionline.org/publications/anonymous-context-politics-and-power-behind-mask/ (cit. on p. 50).

[Com04] Commission of the European Communities. *Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism*. Oct. 2004. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52004DC0702 (cit. on p. 19).

[Com06a] Commission of the European Communities. *Communication from the Commission on a European Programme for Critical Infrastructure Protection*. Dec. 2006. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52006DC0786 (cit. on p. 19).

[Com06b] Commission of the European Communities. *Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society - “Dialogue, partnership and empowerment”*. May 2006. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52006DC0251 (cit. on p. 21).

[Com09] Commission of the European Communities. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - ”Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”*. Mar. 2009. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52009DC0149 (cit. on pp. 21, 22).

[Cox17a] J. Cox. *NSA Exploit Peddlers The Shadow Brokers Call It Quits*. Jan. 2017. URL: https://www.vice.com/en/article/vv7ja4/nsa-exploit-peddlers-the-shadow-brokers-call-it-quits (cit. on p. 54).

[Cox17b] J. Cox. *They’re Back: The Shadow Brokers Release More Alleged Exploits*. Apr. 2017. URL: https://www.vice.com/en/article/5387an/theyre-back-the-shadow-brokers-release-more-alleged-exploits (cit. on p. 54).

[CS16] N. Y. Conteh, P. J. Schmick. “Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks”. In: *International Journal of Advanced Computer Research* 6.23 (2016), p. 31. DOI: 10.19101/IJACR.2016.623006 (cit. on pp. 59, 60).

[DB 18] DB Netz AG. *European Train Control System (ETCS) - Informationen zu ETCS und der Migration zur europäischen Zugbeeinflussungstechnik bei der DB Netz AG*. July 2018. URL: https://fahrweg.dbnetze.com/resource/blob/4119016/461729e9fed0107df85271ba1bbddf8b/etcsbroschuere_2018-data.pdf (cit. on p. 17).

[Eug11] K. Eugene. *The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight*. Nov. 2011. URL: https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/ (cit. on p. 29).

[Eur04] European Community. *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance)*. Mar. 2004. URL: http://data.europa.eu/eli/reg/2004/460/oj (cit. on p. 21).

[Eur08] European Union. *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)*. Dec. 2008. URL: http://data.europa.eu/eli/dir/2008/114/oj (cit. on p. 20).

[Eur13a] European Commission. *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*. Feb. 2013. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013PC0048 (cit. on p. 25).

[Eur13b] H. European Commission. *Joint Communication to the European Parliament, the Council the European Economic and Social Committee and the Committee of the regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Feb. 2013. URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (cit. on pp. 22–24).

[Eur16] European Union. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. July 2016. URL: http://data.europa.eu/eli/dir/2016/1148/oj (cit. on p. 25).

[Eur19a] European Court of Auditors (ECA). *Challenges to effective EU cybersecurity policy*. Mar. 2019. URL: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf (cit. on p. 24).

[Eur19b] European Union. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)*. Apr. 2019. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj (cit. on p. 26).

[Eur22a] European Union. *Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector (Text with EEA relevance)*. Dec. 2022. URL: http://data.europa.eu/eli/dir/2022/2556/oj (cit. on pp. 26, 64, 65).

[Eur22b] European Union. *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)*. Dec. 2022. URL: http://data.europa.eu/eli/dir/2022/2557/oj (cit. on p. 13).

[Eur22c] Eurpol. *European Cybercrime Centre - EC3*. Mar. 2022. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (cit. on p. 23).

[Eur23a] European Cyber Security Organisation (ECSO). *Who we are*. Mar. 2023. URL: https://ecs-org.eu/who-we-are/ (cit. on p. 23).

[Eur23b] European Parliamentary Research Service (ERPS. *The NIS2 Directive - A high common level of cybersecurity in the EU*. Feb. 2023. URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333 (cit. on p. 65).

[EV21] C. Eaton, D. Volz. “Colonial Pipeline CEO tells why he paid hackers a $4.4 million ransom”. In: *Wall Street Journal* 19 (2021) (cit. on p. 49).

[Fil10] J. Fildes. *Stuxnet worm ’targeted high-value Iranian assets’*. Sept. 2010. URL: https://www.bbc.co.uk/news/technology-11388018 (cit. on pp. 30, 39).

[FMC11] N. Falliere, L. O. Murchu, E. Chien. “W32.Stuxnet Dossier”. In: (Feb. 2011). Version 1.4. URL: https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en (cit. on pp. 30–34, 36).

[GBL+18] A. Gabriel, F. Brauner, A. Lotter, F. Fiedrich, O. A. Mudimu. “Cyber security flaws and deficiencies in the European Rail Traffic Management System towards cyber-attacks”. In: *Proceeding of the 15th ISCRAM Conference*. 2018. URL: https://idl.iscram.org/files/alexandergabriel/2018/2108_AlexanderGabriel_etal2018.pdf (cit. on pp. 17, 18).

[GCB+23] I. W. Gray, J. Cable, B. Brown, V. Cuiujuclu, D. McCoy. *Money Over Morals: A Business Analysis of Conti Ransomware*. 2023. DOI: 10.48550/arXiv.2304.11681. arXiv: 2304.11681 [cs.CR] (cit. on pp. 48, 49).

[GJLU23] K. Grauer, E. Jardine, E. Leosz, H. Updegrave. “The 2023 Crypto Crime Report”. In: (Feb. 2023). URL: https://go.chainalysis.com/2023-crypto-crime-report.html (cit. on pp. 51, 52).

[Goo17] D. Goodin. *NSA-leaking Shadow Brokers just dumped its most damaging release yet*. Apr. 2017. URL: https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/ (cit. on p. 54).

[Goo23] Google Threat Analysis Group. *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape*. Feb. 2023. URL: https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf (cit. on p. 44).

[Gre18] A. Greenberg. “The untold story of NotPetya, the most devastating cyberattack in history”. In: 22 (Aug. 2018). URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (cit. on pp. 40, 42, 43).

[Gre19] A. Greenberg. *What Is Cyberwar? The Complete WIRED Guide*. Aug. 2019. URL: https://www.wired.com/story/cyberwar-guide/ (cit. on p. 21).

[Gre20a] A. Greenberg. *Anonymous Stole and Leaked a Megatrove of Police Documents*. June 2020. URL: https://www.wired.com/story/blueleaks-anonymous-law-enforcement-hack/ (cit. on p. 50).

[Gre20b] A. Greenberg. *US Indicts Sandworm, Russia’s Most Destructive Cyberwar Unit*. Oct. 2020. URL: https://www.wired.com/story/us-indicts-sandworm-hackers-russia-cyberwar-unit/ (cit. on p. 43).

[Gri17] A. Griffin. *’Petya’ cyber attack: Chernobyl’s radiation monitoring system hit by worldwide hack*. June 2017. URL: https://www.independent.co.uk/tech/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html (cit. on p. 42).

[Gro11] M. J. Gross. “A declaration of cyber-war”. In: *Vanity Fair* 53.4 (2011). URL: https://www.vanityfair.com/news/2011/03/stuxnet-201104 (cit. on p. 29).

[Gro21] P. P. Groumpos. “A Critical Historical and Scientific Overview of all Industrial Revolutions”. In: *IFAC-PapersOnLine* 54.13 (2021). 20th IFAC Conference on Technology, Culture, and International Stability TECIS 2021, pp. 464–471. ISSN: 2405-8963. DOI: https://doi.org/10.1016/j.ifacol.2021.10.492 (cit. on p. 15).

[Hal10] J. Halliday. *Stuxnet worm is the ’work of a national government agency’*. Sept. 2010. URL: https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency (cit. on pp. 36, 38).

[HKMS12] J. Hull, H. Khurana, T. Markham, K. Staggs. “Staying in control: Cybersecurity and the modern electric grid”. In: *IEEE Power and Energy Magazine* 10.1 (2012), pp. 41–48. DOI: 10.1109/MPE.2011.943251 (cit. on p. 16).

[HSU19] K. Hasan, S. Shetty, S. Ullah. “Artificial Intelligence Empowered Cyber Threat Detection and Protection for Power Utilities”. In: *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*. 2019, pp. 354–359. DOI: 10.1109/CIC48465.2019.00049 (cit. on p. 64).

[Hus13] P. Hustinx. *Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a ’Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace’, and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union*. June 2013. URL: https://edps.europa.eu/sites/default/files/publication/13-06-14_cyber_security_en.pdf (cit. on p. 25).

[IIDE22] I. Ilin, V. M. Iliashenko, A. Dubgorn, M. Esser. “Critical Factors and Challenges of Healthcare Digital Transformation”. In: *Digital Transformation and the World Economy: Critical Factors and Sector-Focused Mathematical Models*. Springer, 2022, pp. 205–220 (cit. on p. 16).

[IS10] P. G. Inglesant, M. A. Sasse. “The True Cost of Unusable Password Policies: Password Use in the Wild”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’10. New York, NY, USA: Association for Computing Machinery, Apr. 2010, pp. 383–392. DOI: 10.1145/1753326.1753384 (cit. on p. 60).

[Kas12] Kaspersky Lab. *Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected*. June 2012. URL: https://www.kaspersky.com/about/press-releases/2012_resource-207-kaspersky-lab-research-proves-that-stuxnet-and-flame-developers-are-connected/ (cit. on p. 39).

[Kel12] B. B. Kelly. “INVESTING IN A CENTRALIZED CYBERSECURITY INFRASTRUCTURE: WHY”HACKTIVISM”CAN AND SHOULD INFLUENCE CYBERSECURITY REFORM.” In: *Boston University Law Review* 92.5 (2012). URL: https://www.bu.edu/law/journals-archive/bulr/volume92n4/documents/KELLY.pdf (cit. on p. 51).

[Kel23] A. Kelley. *Global Appeal of NIST Cyber Framework Leads to Multiple Translations, Possible Updates*. Apr. 2023. URL: https://www.nextgov.com/cybersecurity/2023/04/global-success-nist-cyber-framework-leads-multiple-translations-possible-updates/385758/ (cit. on p. 63).

[Ken08] J. M. Kenoyer. *Indus Civilization*. Vol. 1. Elsevier, 2008, pp. 715–733. URL: https://southasiaoutreach.wisc.edu/wp-content/uploads/sites/757/2017/08/Kenoyer2008-Indus-Valley-Article.pdf (cit. on p. 14).

[KMS12] K. Krol, M. Moroz, M. A. Sasse. "Don't work. Can't work? Why it's time to rethink security warnings". In: *2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*. 2012, pp. 1–8. DOI: 10.1109/CRISIS.2012.6378951 (cit. on p. 60).

[Kov18] E. Kovacs. *US, Canada, Australia Attribute NotPetya Attack to Russia*. Feb. 2018. URL: https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia/ (cit. on p. 43).

[Kre10] B. Krebs. *Experts Warn of New Windows Shortcut Flaw - Krebs on Security*. July 2010. URL: https://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw// (cit. on p. 29).

[KV17] N. Kshetri, J. Voas. "Hacking Power Grids: A Current Problem". In: *Computer* 50.12 (2017), pp. 91–95. DOI: 10.1109/MC.2017.4451203 (cit. on p. 16).

[LA15] I. Lopez, M. Aguado. "Cyber security analysis of the European train control system". In: *IEEE Communications Magazine* 53.10 (2015), pp. 110–116. DOI: 10.1109/MCOM.2015.7295471 (cit. on p. 17).

[Lan11] R. Langner. "Stuxnet: Dissecting a cyberwarfare weapon". In: *IEEE Security & Privacy* 9.3 (May 2011), pp. 49–51. DOI: https://doi.org/10.1109/MSP.2011.67 (cit. on p. 36).

[LB10] G. Lofrano, J. Brown. "Wastewater management through the ages: A history of mankind". In: *Science of The Total Environment* 408.22 (2010), pp. 5254–5264. ISSN: 0048-9697. DOI: https://doi.org/10.1016/j.scitotenv.2010.07.062. URL: https://www.sciencedirect.com/science/article/pii/S0048969710007564 (cit. on p. 15).

[Lee12] D. Lee. *Flame: Attackers 'sought confidential Iran data'*. June 2012. URL: https://www.bbc.com/news/technology-18324234 (cit. on p. 39).

[Lyn20] S. Lyngaas. *Norwegian police implicate Fancy Bear in parliament hack, describe 'brute forcing' of email accounts*. Dec. 2020. URL: https://cyberscoop.com/norwegian-police-implicate-fancy-bear-in-parliament-hack-describe-brute-forcing-of-email-accounts/ (cit. on p. 47).

[Mag03] R. J. Magnusson. *Water technology in the Middle Ages: cities, monasteries, and waterworks after the Roman Empire*. JHU press, 2003. ISBN: 0-8018-6626-X (cit. on p. 15).

[McG12] M. McGuire. "Organised crime in the digital age". In: *London: John Grieve Centre for Policing and Security* (2012) (cit. on p. 50).

[MD22] L. Maschmeyer, M. Dunn Cavelty. "Goodbye Cyberwar: Ukraine as Reality Check". In: *CSS Policy Perspectives* 10.3 (2022). DOI: 10.3929/ethz-b-000549252 (cit. on p. 45).

[Mic10] Microsoft. *Microsoft Security Bulletin MS10-073*. Oct. 2010. URL: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-073 (cit. on p. 31).

[Mic17a] Microsoft. *Microsoft Security Bulletin MS17-010*. Mar. 2017. URL: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 (cit. on pp. 40, 42).

[Mic17b] Microsoft Defender Security Research Team. *New ransomware, old techniques: Petya adds worm capabilities*. June 2017. URL: https://www.microsoft.com/en-us/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities (cit. on pp. 40, 42).

[Mil06] R. Miller. *Hurricane Katrina: Communications & infrastructure impacts*. Tech. rep. National Defense University, Fort McNair, DC, 2006. URL: https://apps.dtic.mil/sti/pdfs/ADA575202.pdf (cit. on p. 14).

[MN16] F. Marquart, B. Naderer. "Communication and Persuasion: Central and Peripheral Routes to Attitude Change: von Richard E. Petty & John T. Cacioppo (1986)". In: *Schlüsselwerke der Medienwirkungsforschung* (2016), pp. 231–242. DOI: https://doi.org/10.1007/978-1-4612-4964-1 (cit. on p. 56).

[MPD19] D. Markopoulou, V. Papakonstantinou, P. De Hert. "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation". In: *Computer Law & Security Review* 35.6 (Nov. 2019), p. 105336. DOI: 10.1016/j.clsr.2019.06.007 (cit. on pp. 25, 26).

[MRHM11] A. Matrosov, E. Rodionov, D. Harley, J. Malcho. *Stuxnet Under the Microscope*. Revision 1.31. Jan. 2011. URL: https://www.welivesecurity.com/wp-content/uploads/2012/11/Stuxnet_Under_the_Microscope.pdf (cit. on pp. 30, 32).

[Nat18] National Institute of Standards and Technology (NIST). *Framework for improving critical infrastructure cybersecurity*. Version 1.1. Apr. 2018. DOI: 10.6028/NIST.CSWP.04162018 (cit. on pp. 61–63).

[NIS] NIST - Computer Security Resource Center (CSRC). *advanced persistent threat - Glossary | CSRC*. URL: https://csrc.nist.gov/glossary/term/advanced_persistent_threat (cit. on p. 47).

[NMT12] E. Nakashima, G. Miller, J. Tate. *U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say'*. June 2012. URL: https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html (cit. on p. 39).

[Pre97] President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures*. 1997. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/critical-foundations-protecting-americas-infrastructures (cit. on p. 18).

[PRO22] PRODAFT Threat Intelligence (PTI) team. *Wizard Spider In-Depth Analysis*. Mar. 2022. eprint: 2304.11681. URL: https://www.prodaft.com/m/reports/WizardSpider_TLPWHITE_v.1.4.pdf (cit. on p. 48).

[PS14] K. Peretti, J. Slade. "State-Sponsored Cybercrime: From Exploitation to Disruption to Destruction". In: *The SciTech Lawyer* 10.2 (2014). URL: https://www.alston.com/-/media/files/insights/publications/2014/03/icyber-alerti-statesponsored-cybercrime-from-explo/files/click-to-view-cyber-alert-pdf/fileattachment/14183statesponsoredcybercrime.pdf (cit. on p. 47).

[PT22] J. Przetacznik, S. Tarpova. "Russia's War on Ukraine: Timeline of Cyber-Attacks". In: *European Parliamentary Research Service (EPRS)* (June 2022), pp. 1–7. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf (cit. on p. 43).

[PwC17] B. PwC UK. *Operation Cloud Hopper*. Apr. 2017. URL: https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-report-april-2017.pdf (cit. on p. 48).

[Rai00] A. K. Rai. "Media at war: Issues and limitations". In: *Strategic Analysis* 24.9 (2000), pp. 1681–1694. URL: https://ciaotest.cc.columbia.edu/olj/sa/sa_dec00raa01.html (cit. on p. 45).

[RH10] A. Renda, B. Hammerli. "Protecting critical infrastructure in the EU". In: (2010). URL: https://www.ceps.eu/download/publication/?id=6906&pdf=Critical%20Infrastructure%20Protection%20Final%20A4.pdf (cit. on pp. 20, 21).

[San12a] D. E. Sanger. *Confront and conceal: Obama's secret wars and surprising use of American power*. Crown, 2012. ISBN: 978-0307718037 (cit. on p. 38).

[San12b] D. E. Sanger. *Obama Order Sped Up Wave of Cyberattacks Against Iran*. June 2012. URL: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (cit. on pp. 36, 38).

[SBP17] P. Schaab, K. Beckers, S. Pape. "Social engineering defence mechanisms and counteracting training strategies". In: *Information & Computer Security* (June 2017). DOI: 10.1108/ICS-04-2017-0022 (cit. on p. 60).

[SGO14] A. N. Singh, M. Gupta, A. Ojha. "Identifying critical infrastructure sectors and their dependencies: An Indian scenario". In: *International Journal of Critical Infrastructure Protection* 7.2 (2014), pp. 71–85. DOI: https://doi.org/10.1016/j.ijcip.2014.04.003 (cit. on p. 13).

[SH17] K. Sood, S. Hurley. *NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft*. June 2017. URL: https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ (cit. on p. 41).

[Sha13] D. Shamah. *Major failures, minor successes for anti-Israel hackers*. Apr. 2013. URL: https://www.timesofisrael.com/major-failures-minor-successes-for-anti-israel-hackers/ (cit. on p. 51).

[SK19] F. Salahdine, N. Kaabouch. "Social Engineering Attacks: A Survey". In: *Future Internet* 11.4 (2019). ISSN: 1999-5903. DOI: 10.3390/fi11040089. URL: https://www.mdpi.com/1999-5903/11/4/89 (cit. on pp. 54, 55).

[Sli20] R. Sliwa. *Disinformation campaigns in social media*. B.S. thesis. June 2020. DOI: 10.18419/opus-11202 (cit. on pp. 44, 47).

[SM+07] K. Scarfone, P. Mell, et al. "Guide to intrusion detection and prevention systems (idps)". In: *NIST special publication* 800.2007 (Feb. 2007), p. 94 (cit. on pp. 63, 64).

[SR22] R. Speidel, R. Robbi. *Electronic certificates of incapacity to work as of January 1, 2023*. Nov. 2022. URL: https://www.bdo.de/en-gb/insights/publishments/tax-legal/electronic-certificates-of-incapacity-to-work-as-of-january-1-2023 (cit. on p. 16).

[SRH15] S. J. Shackelford, S. Russell, J. Haut. "Bottoms up: A comparison of voluntary cybersecurity frameworks". In: *UC Davis Business Law Journal* 16 (2015), p. 217. URL: https://hdl.handle.net/10535/10254 (cit. on p. 63).

[Sto97] G. R. Storey. "The population of ancient Rome". In: *Antiquity* 71.274 (1997), pp. 966–978. DOI: 10.1017/S0003598X00085859 (cit. on p. 15).

[Thi16] S. Thielmann. *DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach*. July 2016. URL: https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2 (cit. on p. 47).

[Tra07] I. Traynor. *Russia accused of unleashing cyberwar to disable Estonia*. May 2007. URL: https://www.theguardian.com/world/2007/may/17/topstories3.russia (cit. on p. 21).

[Und09] P. C. Underwood. "New directions in networked activism and online social movement mobilization: The case of anonymous and project chanology". PhD thesis. Ohio University, 2009 (cit. on p. 50).

[Uni17] United States Computer Emergency Readiness Team. *Malware Initial Findings Report (MIFR) - 10130295*. June 2017. URL: https://www.cisa.gov/sites/default/files/publications/MIFR-10130295.pdf (cit. on pp. 40, 42).

[Uni18] United States District Court Western District of Pennsylvania. *United States of America v. Aleksei Sergeyevich Morenets, Evgenii Mikhaylovich Serebriakov, Ivan Sergeyevich Yermakov, Artem Andreyevich Malyshev, Dmitriy Sergeyevich Badin, Oleg Mikhaylovich Sotnikov, Alexey Valerevich Minin*. Oct. 2018. URL: https://www.justice.gov/opa/page/file/1098481/download (cit. on p. 48).

[Van23] N. Vandezande. "Cybersecurity in the EU: How the Nis2-Directive Stacks Up Against its Predecessor". In: (Mar. 2023). DOI: 10.2139/ssrn.4383118 (cit. on pp. 65, 66).

[Vin17] A. Vincent. "State-sponsored hackers: the new normal for business". In: *Network Security* 2017.9 (2017), pp. 10–12. ISSN: 1353-4858. DOI: https://doi.org/10.1016/S1353-4858(17)30113-7 (cit. on p. 48).

[Wak17] J. Wakefield. *Tax software blamed for cyber-attack spread*. June 2017. URL: https://www.bbc.com/news/technology-40428967 (cit. on p. 40).

[WHD18] S. Walker-Roberts, M. Hammoudeh, A. Dehghantanha. "A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure". In: *IEEE Access* 6 (2018), pp. 25167–25177. DOI: 10.1109/ACCESS.2018.2817560 (cit. on p. 17).

[Wol22] E. Wolfangel. *Ein falscher Klick*. Erstausgabe. München: Penguin Verlag, 2022. ISBN: 978-3-328-10904-4 (cit. on pp. 59, 60).

[Wri22] J. Wrieden. *Who is Trickbot? - Analysis of the Trickbot Leaks*. July 2022. URL: https://www.cyjax.com/app/uploads/2022/07/Who-is-Trickbot.pdf (cit. on p. 49).

[WZS21] Z. Wang, H. Zhu, L. Sun. "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods". In: *IEEE Access* 9 (Jan. 2021), pp. 11895–11910. DOI: 10.1109/ACCESS.2021.3051633 (cit. on pp. 54–57).

All links were last followed on June 13, 2023.

Declaration

I hereby declare that the work presented in this thesis is entirely my own and that I did not use any other sources and references than the listed ones. I have marked all direct or indirect statements from other sources contained therein as quotations. Neither this work nor significant parts of it were part of another examination procedure. I have not published this work in whole or in part before. The electronic copy is consistent with all submitted copies.

---

place, date, signature