UNIVERSITY OF PIRAEUS
Department of International & European Studies
MSc in Energy: Strategy, Law and Economics

Cybersecurity and Energy

The Case Study of Stuxnet

Maria G. Zampati

MEN 20011

Supervising Professor: Dr. Platias, Athanasios

the intellectual work fulfilled and submitted based on the delivered master thesis is exclusive property of mine personally. Appropriate credit has been given in this diploma thesis regarding any information and material included in it that have been derived from other sources. I am also fully aware that any misrepresentation in connection with this declaration may at any time result in immediate revocation of the degree title.

Contents

1. Introduction

Energy is omnipresent in our everyday lives. It is one of the main sources of economic growth, mainly because majority of the production and consumption sector use it to fuel their activities. Therefore, it is one of the most pivotal inputs for the economic development. If we think about it, through using energy, the economic productivity and industrial growth are enforced, while it is of great importance for the operation of modern economies. Some analysists may even argue that a direct cause of a country's GDP growth can be the growth in energy (Asghar, Z., 2008). Therefore, the imperative need for energy security is crystal clear, since any malfunction in the energy system can potentially lead to the paralysis of a country's economic and industrial sector.

Energy security according to academics is a policy problem that stemmed in the early 20th century and was related with the oil supply for armies, but it became a more prominent issue and fleshed-out concept in the 1970s due to the oil crises that took place in 1973 and 1979 respectively. In October 1973 broke out the Arab-Israeli war, also known as the Yom Kippur war, which was initiated by Egypt and Syria against Israel, where the US provided the Israeli forces aid by establishing a supply line to Israel (The Editors of Encyclopaedia Britannica). Therefore, the oil crisis that took place during the years of 1973/74, was a way for the Arab oil producers to punish the West for their support for Israel in the Yom Kippur war, by boycotting the US and imposing an embargo which led to the rise of the price of the crude oil from 3 dollars per barrel to 12 by 1974 (Macalister, T., 2011). The second energy crisis that took place in the 70s and caused oil price shocks, was in 1979, as an aftermath of the Iranian revolution (1978-1979). The situation in Iran generated a huge decline in the global supply of crude oil, since Iran is one of the most important petroleum exporting countries. The overall situation caused by said short-term disruption of supply, brought about a rapid increase in prices and panic buying (Downey, L., 2020). But even though those two crises had a huge impact in the global energy market, the general interest in the topic of energy security decreased during the late 80s and in the 90s, since any imminent threats from political embargoes as well as the oil prices in general got stabilized during that period. It was in the 2000s, when it came back as a concept again

fueled by the various issues in the gas supplies in Europe, the growing demand in Asia and the general pressure for the decarbonization of the energy systems (Cherp, A, and Jewell J., 2014)

But how can we actually conceptualize energy security? Energy security in general is a term that is complex and difficult to describe, since it's entangled with a broad range of spheres, such as the economic, the social, the political, the technical etc. As an abstract idea and more so a concept, in contrast to any policy or a term, it's hard to define "energy security". It's a concept that, in general, can differ according to various and different perspectives. Energy security nowadays has transformed into an interdisciplinary field and has become entangled with other security issues. From these security issues, we cannot ignore those who stem from the new rising domain of cyberspace. With the term "cyber" it's described usually anything that has to do with networks and computers.

Cyberspace as a term was first used by speculative fiction writer William Gibson in his cyberpunk, science fiction novel *Neuromancer*, which was released in 1984. He used it there to describe the world of computers as well as the society that is gathered around them. The fantasy world that was illustrated in the book where the world we live in was one of interconnected computers has nowadays become a reality in the form of the Internet. In this novel, he described cyberspace as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts… A graphic representation of data abstracted from the banks of every computer in the human system (Malik, J. K., Choudhury, S., 2019)". Nowadays, cyberspace has been recognized as the fifth domain of military operations after the land, sea, air and space, with the sole difference being that it is man-made. According to Dr. Daniel T. Kuehl, cyberspace can be now defined as "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies (Kuehl, D. T., 2009)".

More particularly, and during the past decade, attacks in the cyberspace domain have evolved and intensified. But cyberattacks have not been something uncommon even for the energy sector. It can be noted here that the very first cyberattack that was ever

recorded, was one against the energy sector. It was Trans-Siberia pipeline attack, which was the first purported CNA-style cyber operation[1] and took place as far as 1982. Even though it's still an attack clouded by uncertainty, that year a part of the Trans-Siberia pipeline exploded. The source of the explosion was noted to be a computer malware that was implanted by the CIA and caused the malfunction of the SCADA system[2] that ran the pipeline. Even though the Trans-Siberia pipeline attack is still considered alleged, it has to be pointed out that it led to the "most monumental nuclear explosion and fire ever seen from space" and even its significance is of great importance since it was an attack against the energy infrastructure of a country and not an explicitly military in nature. The pipeline that got attacked was that generated a revenue of $8 billion annually, through the transportation of natural gas to western Ukraine and therefore to the broader energy market (Whyte, C. and Mazanec B., 2019).

The main goal of this paper is to analyze how cyberspace and more particularly cyberattacks affect the energy sector and more specifically how the Stuxnet cyberattack made us view security in the energy sector differently. This thesis will firstly analyze the importance as well as the digitalization of critical infrastructure. It will then showcase the difference brought up to the energy sector by the emerging domain of cyberspace. The notion of a cyberattack, the nature of the actors as well as their motives will be also defined. Then the elaborate case study of Stuxnet will follow. The reason the Stuxnet cyberattack was chosen, was because it was the first one that showcased the grave implications a cyberattack can have in the energy sector and critical infrastructure. Later the lessons learned from the Stuxnet cyberattack as well as the resilience measures adopted so far by the United States, the European Union and NATO will be analyzed. Last but not least the conclusion drawn by this analysis will be illustrated.

[1] CNA-style cyber operations are those that are designed to disrupt, damage or destroy computers and computer systems, or are cyber operations controlled by a computer. A case of a CNA-style cyber operation is Stuxnet, which will be later analyzed in this paper (Zetter, K., 2016).

[2] SCADA systems are computer-based mechanisms that control and monitor physical operations. They most of the times consist of network devices like controllers, actuators, sensors and communication devices. Important factors for the operation of SCADA systems are central data acquisition and control over distributed assets (Collins, S., and McCombie, S., 2012).

2. Critical Infrastructure as an Element of Energy Security

The importance of critical infrastructures in the modern society is huge as they provide essential services while at the same time, they are one of the most important factors in economic activities. They are composed of the finance, energy, health, transport, telecommunications and energy sectors; with the energy sector being by far on the most multi-layered and complex ones. That is mainly because other sectors and essential services wouldn't be able to function without the aid of the energy sector. Therefore, the influence the energy sector has both financially and societally is great and just the possibility of potential unavailability in supply in energy – as showcased above with the oil crises – could lead to instability with effects far more long-lasting than just the period the unavailability occurred. Accordingly, in the case of a long-lasting disruption in the energy supply, the society is at a high risk with probable serious effects on its gross domestic product (GDP). It has to be noted here that all these aforementioned challenges apply to all subsectors of the energy sector. These are more specifically, electricity, oil and gas as well as nuclear energy, with the latter being of utmost importance for our analysis (Energy Expert Cyber Security Platform, 2017).

2.1. Changes and Digitalization of the Infrastructure

Even with a short delay in comparison with other sectors, the energy sector has entered as well a digital revolution (Desarnaud, G., 2017). A digitalized energy system can perform tasks such as transmission, network and power generation way quicker and more precisely than any device or system that is dependent on human management (Energy Expert Cyber Security Platform, 2017). Information and communication technologies (ICTs)[3] have been changing the processes of energy production, storage and consumption by being used in the energy infrastructures (Desarnaud, G., 2017).

[3] Information and communication technologies (ICTs) is used as a broader term for Information Technology (IT) and it refers to all communication technologies such as the Internet, cell phones, wireless networks, social networking and various other media services and applications that aid and enable their users to access, retrieve, store and transmit information in digital form (Food and Agriculture Organization of the United Nations).

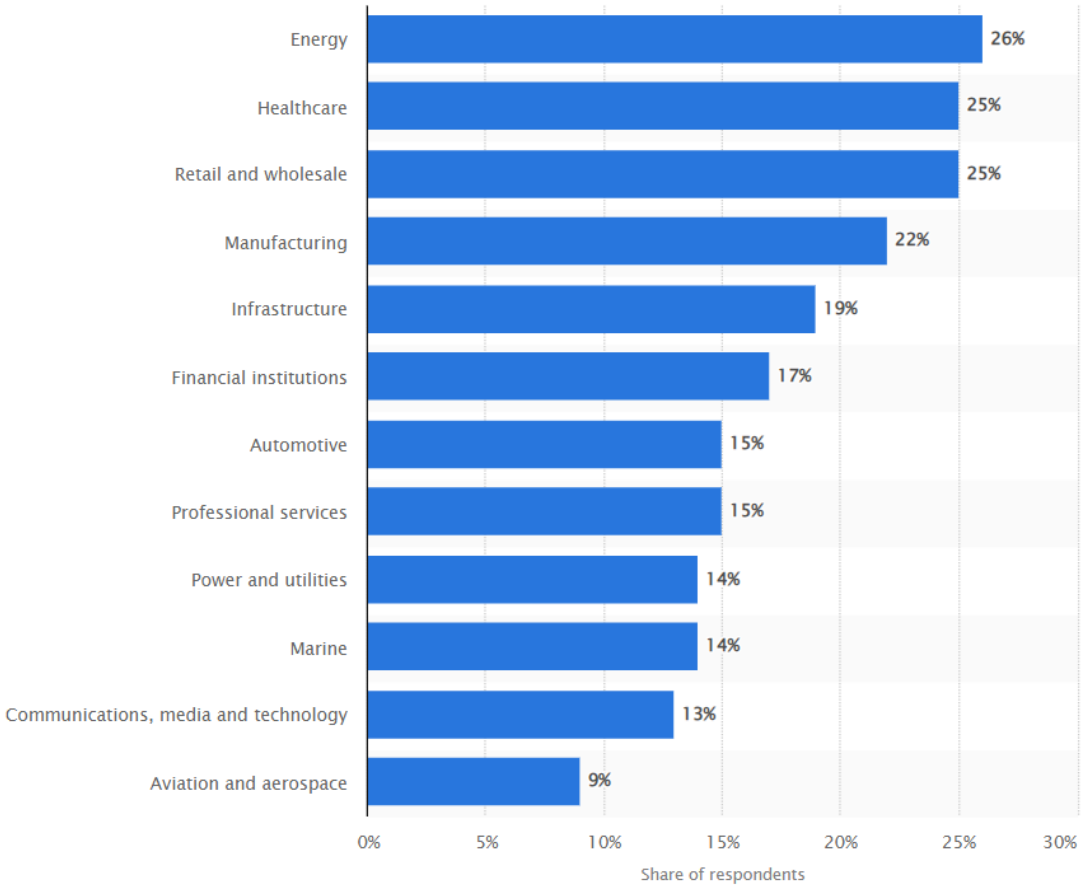
Through this way, the energy management has been optimized and therefore it's easier to have a quicker response to any probable outages.

At this point, the energy industry is composed of both legacy[4] and next generation technologies. In comparison with the past and thanks to the new technologies, the communication of the systems has been developed thanks to the new intelligent components introduced that communicate in more advanced ways. Amongst these new components are the aforementioned ICT that have the ability to be interconnected to local networks and therefore the analog components have been replaced by these digital systems.

The deployment of ICTs in the energy sector was important and needed for three important reasons. Firstly, it was needed in order to facilitate production with the use of tools and instruments that have the ability to collect and process vast quantities of data. Secondly, the imperativeness of sharing information and data with actors, such as management entities and maintenance teams, that are outside of the sector's industrial sites. Last but not least, there was also the necessity to make savings on the software that was used while at the same time enabling the communication between the industrial and management sites (Desarnaud, G., 2017).

As it can be understood, the digitalization of the energy sector has clearly improved the productivity, safety and accessibility of the energy systems, but at the same time it has also brought new security and privacy risks (IEA, 2017). As the following graph will illustrate, as of September 2017, the energy sector has been the prime target of cyberattacks worldwide with 26% (Statista, n.d.)

[4] Through legacy technology are described computer systems that are outdated and unmaintainable software, technologies or programming languages, or that cannot be easily updated or replaced. For a system to be characterized as a legacy doesn't mean that it is defective and many organizations and companies choose to still use legacy systems, since they deem them essential for their daily work (Allan, M., 2019).



Graph 1: Industries impacted by cyberattacks worldwide as of September 2017

Source: Statista, (n.d.)

Before its digitalization, the energy sector, who was mainly using analogue and mechanical equipment, was little exposed to cyber threats, such as cyberattacks and cyber incidents (Desarnaud, G., 2017). But with the emergence and current wide-spread use of ICTs and data communication in the energy sector cyber risks are becoming of critical importance and the possible vulnerabilities of the sector to cyberattacks have increased. That is mainly because the energy industry has been using industrial control systems (ICS)[5] and turnkey operating systems[6], that are not as expensive as others, such

[5] Industrial Control Systems (ICS) were used in order to control and automate various industrial processes. It is used as a general term to define various types of software, amongst them being data acquisition systems (SCADA) and supervisory control. These are control/demand systems that aid and allow remote supervision as well as the control of equipment and plant. They are known to be widely used in the energy sector and are prone to cyberattacks.

[6] A turnkey operating system is a computer system that is given to a costumer in its complete form and therefore can be used immediately. In a sense it can be explained as a “turn the key and go” system (Collins Dictionary).

as proprietary control systems[7], but at the same time are way more vulnerable to malware that can be used through cyberattacks. Furthermore, the equipment and machinery used in the energy sector, might be as old as thirty years and have a lifespan of way more years. This very well shows that all this machinery used even nowadays has been built during the early years of the Internet, when cyberspace was still a domain relatively unknown and concerns over cyberattacks were therefore barely existent. As an obvious result, any protection system for this type of attacks was not in the security functions. Because of that a lot of current, existing vulnerabilities have still not been identified and therefore put the energy industry in extra risk. To add to this, the application of security patches created for software vulnerabilities identified and in general traditional IT[8] security solutions, cannot be easily applied in the industry. It has been argued that the application of an antivirus security patch could unexpectedly lead to machinery shutdowns, while at the same time their functioning can also be altered. Subsequently, to avoid any unwanted implications like the ones aforementioned, majority of the software in the energy industry is rarely ever updated, increasing the risks of cyber threats and cyberattacks, since the machinery is still accessible on the Internet and other public networks (Desarnaud, G., 2017).

2.2. Changes in Cybersecurity and the Energy Sector

In order to support the resilience and reliability of the energy sector in the dawn of a cyberattack, there's been an extra focus in the cybersecurity. Cybersecurity is defined as the implementation of technologies, controls and processes in order to protect systems, devices and networks from cyberattacks, while at the same time it has the goal to minimize the risk of cyberattacks and protect the systems and networks from unauthorized exploitation. When it comes to the energy sector, a big difference between it and the IT sector, is that unlike the latter, the energy sector cannot be easily

[7] A proprietary control system is a system that ingrates with software and equipment exclusively produced by the company that created and manufactured the system (Mid-Atlantic Controls Corp., 2020).
[8] The term IT stands for "Information Technology". It encompasses everything related to computing technology, like hardware, software, networks, the Internet or even the people that work with these technologies (TechTerms).

disconnected from the network, since this could potentially lead to various implications such as burnouts or even blackouts, as it was illustrated above.

When it comes to cybersecurity, there are three main accepted protection goals, which are namely confidentiality, integrity and availability. In contrast when it comes to the energy sector the goal with the highest importance changes according to the industry specific applications.

Aside from the threats aforementioned, considering the vulnerability of the systems and machinery used in the energy sector, it must also be highlighted, that human errors are also extremely common. Sometimes it happens because their training is lacking or because of the fact that the machineries and systems use the same old passwords that remain unchanged and therefore are easier to be hacked. Furthermore, the extensive use of external controllable devices such as USB flash drives, external hard disks, phones and laptops is also a high-risk factor because they can either easily be used to spread malware or at the same time easily getting infected.

Before 2010, even though the risks were there, they weren't thoroughly examined and neither were the protective measures to combat them. The incident that triggered the energy industry's concerns was the discovery of the Stuxnet virus in 2010 in Natanz's uranium enrichment site in Natanz. This analysis will later focus on this particular case, but in general as an incident it proved that the energy sector could experience an attack both its machinery and infrastructures as well as in its management network. Since the energy sector is of pivotal importance to a country's economy, it's therefore a prime target to cyber threats and cyberattacks. In the next section we will analyze the nature of the actors and their motives (Desarnaud, G., 2017).

3. The Energy Sector as a Prime Target: Actors and Motives

First of all, it is important to define what a cyberattack is. It is difficult to give just one definition for the term "cyberattack", since they come in various forms that also have different danger ratings. They vary from basically harmless acts to attacks that are economically significant to even life-threatening strikes (Mortera-Martinez, C., 2018).

They can vary in their motives and methods and amongst their targets can be both state and non-state actors.

Cyberattacks can be categorized in two sub-categories; targeted and untargeted cyberattacks. In the case of a targeted attack, an actor is singled out because the attacker either has a particular interest in its business or because they have been paid to attack said actor. Usually, targeted attacks are more damaging in comparison to non-targeted attacks. This is mainly because in the case of targeted attacks, because they have been tailored specifically to attack a particular system. This category involves methods such as spear-phishing, use of botnets or subversion of the supply chain. More specifically, the case of spear-phishing is when emails are sent to particular individuals that are targeted, that usually contain an attachment or external link that are linked to a malicious software. Furthermore, the deployment of botnets is used to deliver a DDoS attack[9] and the subversion of the supply chain is used in order to attack the equipment or the software that is being delivered to the target.

In the case of un-targeted attacks, the attackers target as many devices, users or services as the can with no discrimination. The nature of the victim has no important role or meaning, since there will be a range of services and machinery with vulnerabilities. In order to achieve this, the attackers exploit techniques that have the ability to take advantage of the openness of the Internet. This category involves methods such as phishing, water holing ransomware and scanning. More explicitly, in the case of phishing we have emails sent to many people asking for sensitive information, like bank details, or including links that lead to a fake, malicious website. Through water holing, a fake website is set up or a legitimate website is compromised in order to attract and exploit its visiting user. Lastly, ransomware attacks, include disseminating disk encrypting extortion malware, while through scanning wide swatches on the Internet are randomly attacked (National Cyber Security Centre, 2015).

Just like the types and methods of cyberattacks can vary, the threat agents behind cyberattacks can vary as well. They can be mainly state and non-state actors. More

[9] Denial of Service (DoS) is a type of cybercrime, that, if successful, forces the website-target to stop its functioning. This is achieved by clouding the target with unnecessary data and information. As a result, the target's users' service is hampered and the website is forced to shut down. DDoS (Distributed Denial of Service) is a type of a DoS attack, in which a lot of computers, that are asking for parallel service from the website-target, are used. These computers belong to a botnet, which the cyber-criminal is usually renting from another same one (Φρυδάς, Ν. Π., 2018).

specifically, the non-state actors can be hacker groups or organized hackers, script-kiddies[10], hacktivists, cyber criminals, insiders, cyber spies and terrorists (Energy Expert Cyber Security Platform, 2017, & EUROPOL, 2018). Out of these threat actors probably the most prominent and dangerous ones are cyber criminals, insiders and hacktivists (EUROPOL, 2018).

Cyber criminals are usually either individuals or groups of people that use technology in order to conduct malicious acts and activities on networks or digital systems with their main goal being to steal sensitive information of a company or personal data in order to gain profit. Cyber criminals most often access cybercriminal underground markets that can be found in the deep web[11] in order to trade their malicious goods and services (hacking tools, stolen data etc.) in order to gain profit. These markets are known to specialize in particular services or products (TrendMicro).

Insiders are individuals or a group of people that launch insider attacks as malicious users that are entrusted with authorized access in a particular system. It has been estimated that 29% of all the reported electronic crimes come from insider attacks and they lead to huge damage. Because an insider, as aforementioned, has authorized access in the system-target as well as extensive knowledge of it, it is subsequently extremely difficult to detect an insider attack and be able to separate it from normal system behaviour in stark contrast with an external attack (Jin X., et al., 2012).

Last but not least, hacktivists are usually groups of criminal hacker groups who come together in order to carry out cyberattacks in order to support political causes. They usually target entire industries but occasionally they attack particular organizations that don't correlate with their political views and practices (Fowler, K., 2016). According to pretty well-known work on the topic, *Hacktivism and the Future of Political Participation* by Alexandra Whitney Samuel, hacktivism is defined as "the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools

[10] A script-kiddie is a low-skilled criminal that uses scripts or programs that are usually developed by others, with not properly understanding how they actually work. They use in a sense ready-made exploit kits or other unrelated programs because they can't create malicious tools of their own. Occasionally, script-kiddies claim authorship of the malware they used by changing its code minimally. It's a very frequent phenomenon amongst game crackers (Kaspersky IT Encyclopedia).

[11] The deep web, which is also often referred to as the hidden web or invisible web, is different from the surface web that can be accessed through the standard search engines. A lot of experts and analysists estimate that the deep web is much larger than the standard surface web. It included websites that are not indexed, private databases, fee-for-service sites and last but not least the dark web (Frankenfield J., 2020).

include website defacements, redirects, DDoS attacks, information theft, website parodies, virtual sit-ins[12], virtual sabotage, and software development (Samuel A. W., 2004)".

3.1. The Motives Behind the Cyberattacks

Before we move on with the analysis of the case study of Stuxnet and after the definition and analysis of what a cyberattack is and who the actors behind one could be, it is important to analyse the motives behind the cyberattacks in the energy sector. They are mainly divided in two categories; namely the financial and geopolitical motives.

3.1.1. Financial Motives

Probably the most common motive behind a cyberattack in the energy sector, is financial gain. Already, there are a lot of financial motives behind wanting to attack the control system of an energy infrastructure, but such a choice could hinder profitability in contrast with just simply targeting a company's management network. Just through the use of a ransomware, lots of monetary profitability can be gained in no time, without even having to aim at critical infrastructures, making cyberattacks in the energy sector extremely appealing (Desarnaud, G., 2017).

Furthermore, unlike IT, just like aforementioned, it is difficult to attack the operational technology infrastructure successfully, since the connectivity is not that exposed and there are various layers and electric grids that are used in order to build a system's architecture. The type of attacks though that are becoming increasingly prominent in the energy sector are those of cyber sabotage or even cyber warfare, since they have become the weapon of choice for many terrorists or even state sponsored groups (Imeson M., 2017).

[12] With the word virtual sit-in, is described a tactic that is usually used by Internet activists in order to hamper or even halt the traffic on a website. The people that participate in a virtual sit-in try to act out a DDoS attack by having thousands of participants access the site-target at the same time, causing traffic overload in order to either slow down the website's performance or make it completely shut down (Weber J.K.).

Another important factor that we have to take into consideration is industrial espionage. The issue here is that it is difficult to copy equipment and plant configuration through espionage software. The targeted plant and equipment's data is usually stored in the corporate networks of a company, therefore the means and resources needed for such an attack are large and difficult to acquire (Desarnaud, G., 2017).

The above illustrates that even though sometimes it might be hard to use particular forms of cyberattacks against the energy sector, it still remains extremely lucrative.

3.1.2. Geopolitical Motives

The energy industry, aside from being targeted for financial reason, it also faces attempts of sabotage, this time for geopolitical reasons. Two of the most prominent cyberattacks in energy sector, namely Stuxnet in 2010 and BlackEnergy in 2015, according to the investigations and analyses conducted, they were state sponsored attacks and not conducted by independent criminal actors or hacker groups (Desarnaud, G., 2017).

Cyberspace is a domain that has become appealing for state actors as a mean to reach their objectives and promote their national interest. Through the Internet, the anarchic state of the world described by the classic realism theory of international relations, has been realized. In the case of cyberspace and since according the theory of realism, not all states are equal in terms of power, there are states that have more capacity and therefore more power in cyberspace than in any other of the traditional domains – sea, air and land – and are able to showcase their power through the cyber domain (Joseph S. N. Jr., 2010). Nowadays, all the more states have the means to conduct cyberattacks according to their capabilities, since the cyber domain has transformed into a strategic tool for the states to gain influence and political advantage.

The use of IT resources against energy infrastructures, could very well be considered as an act of war. This could have deterred the state-assailant from acting, but with one of the main issues of cyberattacks being the difficulty of attribution, allowing the assailants to attack without worry of overt engagement (Desarnaud, G., 2017). The attribution of cyberattacks has technical, legal and political characteristics. When we

talk about political attribution, we have to take into account the political environment, in which the cyberattack takes place and who takes advantage gain from it (Tsagourias, N., 2012). Political attribution is the only type of attribution that can be exercised in the cyberspace domain, but even that is still difficult. In order to have political attribution, the assailants' motives and the geopolitical context must be clearly understood and more so often the motives are unclear and difficult to pinpoint (Romanosky S., and Boudreaux B., 2019).

But, cyberattacks can assuredly lead to diplomatic tensions and a cyber deterrence game, which could change the geopolitical field and the power balance. With everything above mentioned, it is clear that aside from financial motives, the geopolitical motives behind a cyberattack are just as appealing (Desarnaud, G., 2017).

Even though, a lot of cyberattacks might not have been properly detected, in the past decade the cyberattacks against the energy sector have rapidly increased, showcasing the vulnerabilities of the sector. But the first awakening was, as it has been already briefly illustrated, the 2010 Stuxnet cyberattack.

4. The Case Study of Stuxnet

Virusblokada, a Belarusian antivirus company received on the 17th of June 2010 an email from a customer in Iran. According to it, there was a glitch in a machine that kept rebooting itself. When the Virusblokada staff tried to investigate the unusual case remotely with the use of the Internet, they indeed confirmed that they detected a "worm"[13] they had never encountered before that was of surprising size and extremely complex. The malware[14] was discovered that forensic investigators named "Stuxnet" according to a filename in its code (Lindsay, J.R., 2013). More specifically, Stuxnet is a sophisticated, malicious software that is designed in a way that is able to penetrate and establish control in a quasi-autonomous way over remote systems. It's

[13] Worms are self-replicating programs, that do not require another program to aid in the replication process. They are standalone programs which don't require any kind of human interaction in order for an attack to be instigated (Collins S., and McCombie S., 2012).

[14] Malware, also known as **mal**icious soft**ware**, is a hostile and/ or intrusive program that is designed in a way to intrude a computer without the user's consent. There are three major malware categories; namely viruses, worms and Trojan horses (ENISA, & Collins S., and McCombie S., 2012).

representative of a new generation of malware that are characterized as "fire-and-forget" and it can also be used in cyberspace (Farwell, J.P, and Rohozinski R., 2011). It can spread itself through LANs[15] or USB sticks (Cardenas A. A., and Safavi-Naini R., 2012). In comparison to similar worms, Stuxnet is larger in size and also written with the use of various different programming languages with some encrypted components. It was a worm that was created in order to cause irrevocable damage to Iran's centrifuges, that were used for its nuclear programme, through SCADA systems[16]. More particularly it aimed to target the programmable logic controllers (PLC)[17] and more specifically those used for the control of the centrifuges responsible for the uranium enrichment (CSS, 2017). The way the Stuxnet malware agent was deployed was in the form of a multi-stage attack. The first stage needed the design and creation of a computer code with the purpose to be installed into the facility's computers; namely a beacon. The main role of the beacon was to map out the uranium enrichment plant of Natanz and identify how the centrifuges were controlled by the computer systems. After the beacon would have successfully completed its task, it would use the Internet and the computers it had infected to "report back home". In order to mask the traffic caused by the data transmission back to the Stuxnet control and command servers, two fake soccer related websites were set up that made the web traffic seem as if it were a legitimate fan activity. Then the payload portion of the worm infected the Natanz plant and discreetly entered the computer network and the pre-designated PLCs (Lendvay R.L., 2016). Symantec researchers stated that every day there were up to 9000 new infections caused by Stuxnet. Once the worm was finally inside the nuclear control systems, it would cause the centrifuges used for the uranium enrichment process to spin out of control – just like it was noticed in the beginning – and subsequently they would be destroyed (Collins S., and McCombie S., 2012). It took advantage of a previously unknown LNK vulnerability of the Microsoft Windows operating systems, that is now

[15] A LAN (Local Area Network) is a collection of devices that are bound together in one physical location. Its size can vary from small to large, since it can range from a home network that has one user to an enterprise network that it consists of thousands of devices and users. LAN's main characteristic though is that it connects devices that are located in the same, limited area, unlike a WAN (wide area network) or a MAN (metropolitan area network) (CISCO).

[16] SCADA systems (Supervisory Control and Data Acquisition Systems) are computer-based mechanisms used to control and monitor physical operations. The acquisition of central data and the control over distributed assets are of great importance for their smooth operation (Collins S., and McCombie S., 2012).

[17] PLCs are small computers that are within SCADA systems and control the functions executed by the electrical hardware like timers, relays and witches (Collins S., and McCombie S., 2012).

widely known as the "zero-day vulnerability" (Collins S., and McCombie S., 2012). It is rather difficult and most likely not feasible to pinpoint exactly how Stuxnet was designed and developed, but what is for sure is that it most definitely demanded a considerable amount of manpower, resources and time (CSS, 2017).

As illustrated above, the main target of Stuxnet was the Iranian nuclear plant and uranium enrichment site that was located in Natanz. Natanz's cascades are all arranged in 164 centrifuges and at the same time Stuxnet was programmed to attack devices that were organized in groups of 164 objects, making it hard to believe that it was just a coincidence. It is believed, that the Bushehr power plant may also have been a major target, but it requires a dissimilar configuration of centrifuges since it used in plutonium enrichment. Furthermore, the centrifuges used in Iran, are the IR-1 European model from the late 1960s and 1970s, making them in the current day and age fairly inefficient and outdated and therefore fragile and more receptive to cyberattacks. Just an abrupt change of speed could cause severe damage. This vulnerability was taken into consideration by the designers of Stuxnet and they exploited it (CSS, 2017). Various security experts have described Stuxnet in their analyses as "the most technologically sophisticated malicious program developed for a targeted attack to date" and also as "a precision, military-grade cyber missile." This cyberattack with the code-name "Olympic Games" managed to destroy more than thousand centrifuges in the uranium enrichment facilities in Natanz (Lindsay J.R., 2013). Natanz's nuclear plant is a closed and air-gapped computer network and therefore it is not connected to the Internet or other networks. Taking this circumstance into consideration, it can be concluded that the network was probably infected by Stuxnet through the use of a USB drive. This also means that the people behind the design and creation of Stuxnet had to have sent person to "deliver" the worm and infect the network like that (CSS, 2017). But to this day it has still been undecided how exactly Stuxnet managed to invade the nuclear uranium enrichment centrifuges.

Opposing to the idea that a USB drive was used in order to infect them, there's also the suggestion that worm infected the ICSs[18] via moving through computer networks. Stuxnet has the ability to take whatever path needed in order to reach its intended

[18] ICSs (Industrial Control Systems) are command and control networks that are created and designed in order to aid and support industrial processes. Probably the biggest subgroup of ICS is SCADA systems. ICS have transformed from isolated and proprietary systems to open architecture systems which are strongly interconnected with the Internet and other corporate networks (ENISA).

destination. According to this notion, Stuxnet could have spread not only though USB drives, but as well through devices that support them, such as printers and scanners. It also must be noted that once Stuxnet infected the system, it initially only attacked three additional computers after the primary one, showing restraint. This was most likely done in order to reduce the worm's visibility and therefore the probability of it being prematurely noticed. This characteristic of the attack showcases that the attacker was not a casual cybercriminal or hacker, since it showcases high professionalism from the malware code authors and designers. ICSs use a special code in order to properly function and run on embedded systems like the PLCs, which are usually controlled by computer systems that use Windows and are not connected to an internal network or the Internet. In an optimal practice setting, an ICS wouldn't be connected to the Internet but in modern ICSs and SCADA systems become all the more interconnected and subsequently are offering pathways from the outside world to PLCs. Therefore, it would be hard, according to this notion, to believe that there's an actual "air-gap" between ICSs and corporate networks. Since information exchanges between the systems become all the more essential, intranets[19] are essential for the proper function of facility and corporate operations (Collins S., and McCombie S., 2012).

According to General Michael V. Hayden, former director of the General Intelligence Agency (CIA) and the National Security Agency (NSA), Stuxnet was "the first attack of a major nature in which a cyberattack was used in order to cause physical destruction" (Lindsay J.R., 2013). The main target behind the Stuxnet cyberattack seemingly was the delay of Iran's nuclear program (IISS, 2011). Many experts from the antivirus field have argued that only a state could be behind the creation and development of Stuxnet due to the fact that it is a worm of high complexity level that requires resource investment. Aside from that a huge factor that alludes to the fact that Stuxnet is a "state-made" worm is that it was created to specifically target and attack the uranium enrichment centrifuges in Natanz. What we can take for given is that the designers of Stuxnet had substantial knowledge concerning the Iranian machines, computer programs and facilities. Iran accused the West and more specifically NATO for the

[19] An intranet is essentially a private network that can only be accessed by authorized users. It is created for internal communications, just like the prefix intra implies. Some intranets can be accessed through the Internet, while others are limited to a particular LAN (local area network). As expected, local intranets are way more secure as they can only be accessed from within the network (TechTerms).

attack. At the same time, experts pinpointed that the evidence and the motive support the idea that the USA and Israel as the perpetrators. (CSS, 2017).

US officials, when speaking on the classified effort with the code-name "Olympic Games", stated that the Stuxnet worm first developed during Bush's administration in 2006 and its main goal was to slowly damage the nuclear capability of Iran while at the same time creating confusion in the circles of Iranian scientists concerning the cause behind the mishaps at the nuclear plant (Nakashima E., and Warrick J., 2012). As illustrated by New York Times journalist David E. Sanger, Stuxnet is probably a malware that was created and launched in order to be used in the operation "Olympic Games" (CSS, 2017). Operation "Olympic Games" is a collaborative effort between CIA, NSA and Israel, according to US officials. In January 2011, the New York Times announced that Stuxnet was created and tested in Israel, in collaboration with the United States, and even though Israeli officials denied making any comment on the claim, as reporters described "they had huge smiles on their faces when asked whether Israel was behind the cyberattack or if they had any knowledge of who was behind it" (IISS, 2011).

Opposing to this view, according to Farwell and Rohozinski, the patchwork design of Stuxnet suggests that behind its development could be at least for a part the cybercrime sector and more specifically the Russian offshore programming community. As they illustrate, parts and elements of Stuxnet's code share the same design with code written by the cybercrime community. They agree that USA could still be Stuxnet's main developer, but state that it could have outsourced the creation of particular parts of the worm to these groups (Farwell P. J., and Rohozinski R., 2011). There is still the possibility that Russia is also the one that perpetrated the attack. To support this claim, it's important to pinpoint, that Russian workers had access to Iran's nuclear facilities. That is possible, because od the Russo-Iranian cooperation at the Busher nuclear site. Russia's probable motive behind the attack is most likely the prevention of Iran from the enrichment of its own uranium. That way Iran would still have to buy enriched uranium with Russia, as it would be left with no other plan to supports its nuclear program (CSS, 2017).

There will always be uncertainties when it comes to pinpointing the perpetrator behind cyberattacks and that is exactly the reason why attribution in cyberspace is a difficult task (CSS, 2017). Attribution in the cases of cyberattacks entail technical, political and

juridical elements. When it comes to the political elements it is important to analyze the political environment in which the attack takes place (Tsagourias N., 2012). Furthermore, in order to attribute any kind of cyberattack, the benefit of the possible perpetrator – cui bono[20] – is one of the biggest indicators (CSS, 2017). Political attribution requires the good understanding of the of the geopolitical context and the perpetrator's motives. But it is pretty difficult, if not actually impossible, to prove that a seeming perpetrator is actually the actor behind the attack. The political motives are not always clear and distinct. Non-state actors, which are frequently used to act out he cyberattacks are usually controlled by particular states in various levels. But at the same time, it is difficult to prove that the state had knowledge or control of the attack (Boudreaux B., and Romanosky S., 2019). When it comes to the case of Stuxnet, majority of the evidence found proves that the United States where probably the main actor behind the development and release of the worm. The US could have achieved with the use of Stuxnet the delay of Iran's uranium enrichment program while at the same time avoided a possible warm war between Israel and Iran. But even with the existence of all these indicators, the possibility of Russia's and/ or Israel's involvement should not be dismissed. Just like in the case with covert operations, similarly in cyberattacks, nothing can be confirmed without any doubt (CSS, 2017).

In order to understand the strategic importance of Stuxnet, it is important to understand it and appreciate it for what it is not. Even though portrayed as such, the worm "Stuxnet" is not as sophisticated and technologically advanced as it has been coined. One of its basic technological characteristics is a DNS-based command and control network that makes the worm less covert than a lot of the more advanced malware used by cybercriminals. Stuxnet could be very well described as Frankenstein patchwork of already existing code, tradecraft and best practices drawn from the global cybercrime community and less likely to be categorized as an autonomous and technologically advanced research programme, making it in reality not than innovative. What in actuality made Stuxnet truly strategically important and unforeseen is the insight is provides about the evolution of computer warfare (Farwell P. J., and Rohozinski R., 2011) as well as the various impacts and effects it had specifically in Iran and in a

[20] Cui bono is ancient Latin and translates into "to whose benefit" in English.

second analysis about the security of critical infrastructures internationally and more specifically of energy infrastructures.

The effects the Stuxnet cyberattack had were various; such as political, economical, social and technological. First of all, it rendered the Iranian government inadequate to protect its nuclear infrastructures from a foreign cyberattack. It was noticed that Iran's government was found indecisive as to how to react to the possibility of a computer worm infecting their nuclear facilities. In November 2010 they even had to admit that the worm might have been active in their nuclear plants for probably more than a year. Furthermore, even though the Iranian government pointed the fingers to the West and more specifically the US for the attack, at the same time they couldn't retaliate because such thing cannot be easily proven and therefore legally attributed. But said inaction made Iran at the same time look incompetent and mayhaps even an easy target. The attack itself did not have any direct effects to the population of Iran or its society. It was an attack that ended up having no collateral damage. Had it ended up otherwise, there could have been way grave effects, as important as the potential use of human lives. Stuxnet's biggest impact in the society is most probably the rising feeling of insecurity. The Iranian citizens saw an internal intrusion with serious effects leading them to probably a lot of doubt concerning the state's cybersecurity measures. Even though as aforementioned the Natanz uranium enrichment site is air-gapped, the perpetrators still found an effective way to invade it, showcasing that no matter how close a network is, it can never be secure enough. Even though the Stuxnet attack was against Iran, it led a general feeling of insecurity globally, especially since the worm managed to spread to other computers around the world (CSS, 2017)..

The Stuxnet cyberattack had direct economic effects for the Iranian state as well. Iran is a state that was subjected to international embargoes and subsequently is doesn't have the access and therefore the ability to buy the needed materials and resources for its nuclear program from the international markets. Since, they cannot buy them they have to build them themselves with sometimes even having to use foreign components. This leads to a patchwork of materials that is not of the best quality and most likely technologically outdated as well, as showcased above, making this one of the reasons for the centrifuges' quick deterioration. So, taking Iran's already limited resources as well as the destruction of circa 1000 centrifuges, it's easy to assume that the cyberattack led to additional pressure concerning stocks of materials and budgets. Aside from this

the worm's attack had long-term economic consequences for Iran as well, since it now had to deal with the management of the delays in production of low-enriched uranium[21]. Moreover, Iran in order to avoid a similar cyberattack in the future also had to invest a lot in new security and especially cybersecurity measures, which definitely require a huge budget, which was a lot for the already deteriorating Iranian economy to handle. Notably here, in November 2011, Iran created a new cyberunit in the context of the Revolutionary Guard Corps[22] in order to address the issue of cyberattacks (CSS, 2017)..

From a technological point of view, the most direct as well as the only physical effect of the Stuxnet attack was the destruction of almost thousand centrifuges. More particularly the worm affected the speed of the centrifuges, making it alternate from fast to slow. This particular change in speed was hidden by the malware's rootkit[23] making it seem as if the operation and speed of the centrifuges was normal. The constant change in speed would lead to the faster deterioration of the centrifuges while at the same time causing damage that would be beyond repair. This way, like aforementioned, Iran had to replace around 1000 centrifuges. Furthermore, the cyberattack had a direct affect on the technology sector. The companies that had produced software that was easily exploitable or with vulnerabilities showcased through the Stuxnet attack had to take action. Particularly, Microsoft had to issue patches that would come as a solution to the zero-day vulnerabilities found in its operating system, while at the same time Siemens created patches too while at the same time offering removal tools for its customers so that the latter could remove the worm from their computers. Moreover, the Stuxnet attack made the Iranians look at any possible malfunction in their nuclear facilities with a high degree of suspicion, since it could very well be another cyberattack.

[21] Low-enriched uranium is one of the basic materials to create nuclear fuel. It is created through the enrichment of naturally occurring uranium in order to amplify its ability to produce energy. The enrichment increased the concentration of uranium atoms that are able to split in order to produce heat. The latter in its turn is used for the electricity generation (IAEA).

[22] The Islamic Revolutionary Guard Corps, also known as Pasdaran, is a part of the armed forces of Iran and independent from Iran's regular army, the latter also known as Artesh. It was founded after the Iranian Revolution (1978-1979), in April 1979 by Iran's former leader Ruhollah Khomeini. After its participation in the Iran-Iraq War (1980-1988), its role got expanded, making it Iran's main military force, having its own army, air and navy force as well as its own intelligence branch (Editors of Encyclopaedia Britannica, 2022).

[23] A rootkit is a type of malicious software that has the ability to infect the hard drive of a computer and allow that way unauthorized "root-level" control and access of the infected computer. Usually, it is hard to wipe off the rootkit without completely erasing the hard drive and having to install again the operating system of the computer. The rootkit can usually get installed through a phishing attack, where the personal computer's owner opens a seemingly trustworthy file that ends up in actuality installing the rootkit (Editors of Encyclopaedia Britannica).

Because of this they managed to find out two different malwares operating covertly in their facilities; namely Duqu[24] and Flame[25] (CSS, 2017)..

Last but not least, the Stuxnet cyberattack had also important effects on an international level. Through this attack the uranium enrichment program of Iran was successfully delayed for a short period of time, taming the at the time international tensions. The delay let Israel feel reassured because it wouldn't have to end up launching an airstrike in order to stop Iran's uranium enrichment physically. Moreover, it was an attack that showcased that even air-gapped energy infrastructures are not enough to make a system be consider fully secured from cyberattacks, creating a dire need for proper cybersecurity measures to be taken. This is why a lot of nations, aside Iran, started updating, reviewing and creating new cybersecurity strategies in order to protect their physical critical infrastructures as well as reinforce their legal abilities to retort to cyberattacks (CSS, 2017). The worm's technical performance showcased that cyberweapons exist, are a real threat and not mere science fiction constructions. It was a fleshed-out proof that ever-present digital technologies can serve as a new form of warfare (Lindsay J.R., 2013). It was, also, an attack that showcased as well that a cyberattack can have real and feasible effects in the real world, creating a worldwide sense of insecurity. Considering Stuxnet's capabilities, the Stuxnet cyberattack could be considered an attack equal to a conventional armed attack. The latter opinion is strengthened by Rule 69 of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, which states that "*a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force*" (International Group of Experts, 2017). Lastly, the fact that the worm managed to spread to computer systems outside of Iran, indicates that anyone with the needed know-how, that could stumble across it, would be able to redesign it by reverse-coding it so that it would fit new purposes or targets. Even the possibility of a terrorist group of finding it and using it that way creates great concerns. Therefore, the need to

[24] Duqu is a sophisticated Trojan that is seemingly created by the same people behind Stuxnet's design. It is used to serve as a backdoor into a system in order to make data theft of private information easier. That is also its main difference with Stuxnet, which was designed for sabotage in critical infrastructures. Also, unlike Stuxnet it cannot replicate on its own (Naraine R., 2011).

[25] Flame is a malicious software that makes Stuxnet size-wise in comparison. It was a different composition and purpose and it also doesn't have probably the same programmers. It's complex nature though, as well as its geographic scope showcase strongly that it is most likely nation-state behind its creation and not the usual cybercriminals. This is the reason why it is considered one of the main tools in the evolving cyberweapon arsenal (Zetter K, 2012).

be able to effectively defend systems and critical infrastructures from such cyberattacks have become a big priority in states' defense policies and strategies (CSS, 2017).

Taking this case study into consideration, it is crystal clear that the Stuxnet cyberattack against Iran's uranium enrichment facilities, illustrated that, critical infrastructures and in particular those of the energy sector or not immune to cyberattacks even if they are completely air-gapped systems. Stuxnet was a rude awakening and the first modern day cyberattack against the energy sector, showcasing the need for cybersecurity and resilience measures.

5. Lessons learned and building resilience

Stuxnet is probably the first publicly recognized cyberweapon that was used in order to attack industrial machinery. It serves as the blueprint, showcasing how an innovative cyberattack with a particular target on computer systems of a CI target should be conducted. With Stuxnet serving as the opening of a Pandora Box of cyberattacks against critical infrastructures as well as the inherent vulnerabilities of the ICT systems showcase the need for cybersecurity measures on a global scale.

5.1. Stuxnet's implications for cybersecurity and critical infrastructures

The Stuxnet cyberattack and its aftermath showcased clearly for the first time that critical infrastructures and the energy sector are at risk of potential cyberthreats. As it has been illustrated in the aforementioned case study the fact that an air-gapped computer network, like the one at the Natanz uranium enrichment plant was not a sufficient enough security measure to protect it from potential cyberattacks (CSS, 2017). Furthermore, Stuxnet challenged the preexistent notion concerning environments that are not connected to the Internet and the assumption that facilities and infrastructure are fully protected from any possible vulnerabilities in software applications. SCADA/ICS personnel had a rude awakening, after the Stuxnet cyberattack, that no computer system is covert or obscure enough to be deemed untraceable or unidentifiable by possible

attackers. Any system can be found, identified, analyzed and subsequently exploited due to their vulnerabilities. The Stuxnet attack illustrated that the attackers probably knew more about the computer system's hardware and software in Natanz than its actual owners (Collins S., and McCombie S., 2012).

It is understandable that states would now wish to focus more on creating cybersecurity measures in order to avoid cases like Stuxnet. Stuxnet showcased that, if we take as a given the scenario that the cyberattack was conducted with the use of a USB stick, a mere USB stick is enough to target networks that are completely air-gapped. Another important measure that should be taken is for states to create a standard procedure that should be easy and adequate and that would be carried out in every future cyberattack case.

Stuxnet was just the beginning for a plethora of various other cyberattacks that came in the next years against the energy sector. For our analysis we will briefly mention three of them; namely Shamoon (2012), Energetic Bear (2014) and BlackEnergy (2015).

5.1.1. Shamoon

Only a couple of years after the Stuxnet attack, the second main cyberattack against the energy sector took place; namely the Shamoon cyberattack. In August 2012, Saudi Aramco, one of the world's biggest state-owned oil companies, got attacked with around thirty-five thousand of its computers having their data completely deleted. The Shamoon malware stole the passwords, erased data and stopped computers from rebooting themselves (CFR). A hacker group with the name "Cutting Sword of Justice" took the responsibility behind the cyberattack. Intelligence officials from the United Stated have considered the probability that the actual instigator of the attack was Iran, but they didn't have enough evidence to back up their claim. Nonetheless, no one has to this date revealed the names behind the attackers. As a result of the Shamoon cyberattack, Saudi Aramco had to completely shut down their internal corporate network, disable Internet access and the employees' e-mails, in order to halt the virus' spread through their network. Aramco expressed though that the core business of exploration and oil production was not hindered or affected in any way by the attack, since as they claimed they depend on isolated network systems (CCDCOE).

5.1.2. Energetic Bear

Two years after the Saudi Aramco Shamoon cyberattack, in 2014, 250 energy companies located in the United Stated and Western Europe got infected by a virus fairly similar to Stuxnet, named Energetic Bear. There are speculations that the worm might have been active since 2011 and its main targets were electricity producers, equipement manufacturers and also oil and electricity distributors. More specifically, the Energetic Bear worm aided the attackers to take control over various industrial equipement. The group that is seemingly behind the virus creation and the attack reportedly infected three industrial control system manufacturers which would have then transmitted the virus to their energy consumers through upgrades and maintenance operations (Desarnaud, G., 2017).

5.1.3. BlackEnergy

On the 23 of December 2015 a cyberattack that took its name from the BlackEnergy malware took place against Ukraine (Styczynski J. and Beach-Westmoreland N., 2019). BlackEnergy is a Trojan Horse DDoS, that became known in 2008 during the conflict between Russian and Georgia and was originally used for DDoS attacks, spam distribution and bank frauds (Paganini, P., 2016). For this specific cyberattack against Ukraine the BlackEnergy 3 edition of the malware was used, which is specifically designed to give unauthorized access to networks. The perpetrators after infecting the network, used legitimate user credentials in order to move within internal systems, ultimately shutting down the electricity distribution. Ukraine's physical infrastructure got a severe hit, since the cyberattack's main targets were three state-owned electricity distribution companies; namely Prykarpattyaoblenergo, Kyivoblenergo and Chernivtsioblenergo and therefore blackouts were caused for more than 225,000 Ukrainian costumers (Styczynski J. and Beach-Westmoreland N., 2019). Simultaneously with the DDoS attacks, there was also a malfunction in Kyivoblenergo's telephony networks (Assante M., 2016). The attackers managed to change the security measures and disable the communication channels, elongating the

blackouts and hindering the damage restoration attempts in for the reinstatement of the systems regular operation (Shackelford S.J. et al, 2017). This particular cyberattack is of great importance, since it was the only one to cause real-time kinetic effects (Whyte C. and Mazanec B., 2019) as well as the first on to achieve the instigation of energy blackouts in various cities simultaneously (Styczynski J. and Beach-Westmoreland N., 2019). This is a cyberattack that just like Stuxnet, is considered to have a nation-state as its perpetrator and in this case the Russian Federation.

These shortly analyzed cases of cyberattacks against the energy sector after Stuxnet showcase that Stuxnet began a new era of attacks in the cyberspace realm, underlying the need for increased protection against cyberthreats and higher cybersecurity standards in critical infrastructures and especially the energy sector. In order to achieve that a more intense cooperation of governments and both public and private actors, who are in control of these infrastructures, is needed. This way it would be possible to build stronger resilience against cyberattacks and any form of threat in the cyberspace sector.

5.2. Building Resilience

Resilience to cyberattacks and cyber-risks is a topic that needs a cross-industry and risk-based approach from both governments and companies alike. For a cybersecurity framework to properly work it should aim at the creation of a cybersecurity culture. In order to achieve this, both national and international cooperative efforts should be included in order to create processes that will combine business, education, legislation and technology approaches to address cyber risks (Teplinsky, 2013).

The Stuxnet attack as well as the briefly mentioned BlackEnergy cyberattack showed that there were actually numerous measures that could have aided for their detection. The principle “defense in depth” helps in the protection of information systems and guarantees that there will be multiple layers of defenses so that the attacker would have to deal with a new security layer after having overcome the previous one. Furthermore, there are basic security principles and measures such as the installation of firewalls, the change of the default passwords of PLCs as well as their frequent change, the separation of operational information systems and management and last but least the application of drastic “hygiene” procedures that aid in the reduction of risks. These basic “hygiene”

procedures are namely the prohibition of connection for any unidentified device or doing a trial use of any new equipement before its installation. The organization behind cybersecurity could someone say that it is probably the main key to success (Desarnaud, G., 2017).

This is the reason why, individual governments as well as union forces such as the European Union (EU) and the North Atlantic Treaty Organization (NATO) have highlighted the importance of cybersecurity of critical infrastructure and more specifically energy infrastructure and also adopted measures to help in protection from cyberthreats. In this thesis we will mainly focus on some of the strategies adopted by the US, the EU and NATO.

5.2.1. United States of America

The Stuxnet cyberattack caused a great sense of insecurity for the US government as well as its private sector underlying the need for coordinate and cooperate practices between the two in order to protect its critical infrastructure US's Department of Homeland Security (DHS) highlights that the key to protect and ensure "homeland security" is to focus on further developing cybersecurity while ensuring resilience in cyberspace. That is mainly because, the reliance and use of technological means in critical infrastructure operations and procedures will only increase (Lendvay R.L., 2016). Therefore, the US government has adopted measures of response against cyberthreats, while at the same time recognizing cyberspace as the fifth domain of warfare (Flowers A. and Zeadally S., 2014).

Even as early as June 2009, the former Secretary of Defense, Robert Gates, had commanded the US Strategic Command (USSTRATCOM) to create a new cyber-focused sub-command. With the events of Stuxnet taking place in June 2010, Gates' memo found a valid pretext and in October 2010 the United States Cyber Command (USCYBERCOM) was founded under USSTRATCOM. USCYBERCOM's mission is to "plan, coordinate, integrate, synchronize and conduct activities in order to direct operations and defense of Department of Defense information networks and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the

same to our adversaries" (U.S. Cyber Command). Even though USCYBERCOM is of clear military nature, it highlights that the events of Stuxnet made the US take strong action in order protect itself from future cyberattacks.

About 85% of US' critical infrastructure is owned by the private sector and therefore, it is evident that the cooperation between private and public sector is of vital importance (U.S Government Accountability Office, 2006). DHS has taken up the role of safeguarding US' critical infrastructure from cyberattacks. It has the leading role in coordination of sector specific agencies, private sector partners and federal agencies in order to promote and strengthen information sharing about cyberthreats and possible vulnerabilities as well as to create a better understanding of the interdependency of infrastructure systems with the entire nation (Cybersecurity and Infrastructure Security Agency, 2021). In 2018, Cybersecurity and Infrastructure Security Agency (CISA) was established under DHS, in order to "work across public and private sectors, challenging traditional ways of doing business by engaging with government, industry, academic and international partners" (Cybersecurity and Infrastructure Security Agency). Furthermore, the DHS in partnership with the critical infrastructure community has created a voluntary program, namely the Critical Infrastructure Cyber Community C^3 Voluntary Program (C^3PV), in order to reinforce the cybersecurity of critical infrastructure. C^3PV's goal is to support the industry's cyber resilience, raise awareness as well as make use of the Framework for Improving Critical Infrastructure Security and also motivate the various organizations to include cybersecurity to their risk management approach. There's also the National Infrastructure Coordinating Center (NICC) under the DHS National Operations Center, which is an information sharing and coordination center that "maintains situational awareness of US' critical infrastructure for the government. It serves in a sense as an information sharing hub for cyber resilience and are aiding in the strengthening of US government's effectives to protect its critical infrastructure (Cybersecurity and Infrastructure Security Agency, 2021). Lastly and maybe the focal key to US' national strategy for securing US government and private sector Industrial Control Systems (ICS) is the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). It serves as investigatory body of ICS incidents, conducts vulnerability analyses and provides onsite response services. Moreover, it aids in the coordination of information sharing between state, federal and local agencies, the intelligence community as well as the

private sector in order for all the stakeholders to work in coordination (Lendvay R.L., 2016).

Now more particularly on the energy sector, the United States have founded the Office of Cybersecurity, Energy Security and Emergency Response (CESER) in order to address current and future emerging threats by improving the security of energy infrastructure as well as aiding the Department of Energy. In case an incident takes place, CESER aids with the coordination between the government and the energy sector with its main aim being the mitigation of the impact of energy disruptions (Office of Cybersecurity, Energy Security, and Emergency Response). CESER regards cybersecurity as highly important and views cybersecurity solutions as a necessity for reliable energy delivery. Stuxnet back in 2010, already proved that cyberweapons are enough to even penetrate and isolated, air-gapped network system, showcasing that it unrealistic to view energy delivery systems as completely isolated or immune to any probable cyberattacks. CESER facilitates the communication between the private and public sector in order for the design and creation of next generation cyber-resilient energy delivery systems and components. CESER has also established the Cybersecurity for Energy Delivery Systems Research and Development Program (CEDS-R&D) in order to help the energy sector owners. This is achieved with the establishment of cybersecurity solutions for energy delivery systems through research and development. CEDS-R&D aligns all activities with the strategy expressed in the Roadmap to Achieve Energy Delivery Systems Cybersecurity as well as with the Federal priorities. Every couple of years, CESER runs a peer review of research partnerships in order to give stakeholders and management unbiased assessments and improvement recommendations (Office of Cybersecurity, Energy Security, and Emergency Response).

Last but not least, it is important to note that on the 12th of May 2021, current president of the United States, Joe Biden, issued and Executive Order for the improvement of the country's cybersecurity. This particular executive order gave strong emphasis to the importance of the development of the US energy sectors cybersecurity (Finite State, 2021).

5.2.2. The European Union (EU)

The European Union has gradually started implementing the needed requirements for cybersecurity in its legislation. In comparison to the aforementioned United States, which started focusing more intensively on security measures against cyberthreats only a few months after the Stuxnet attack, the EU started only in 2016 to do so. In autumn 2016, thought, the European Commission published the Winter Package; namely the Clean Energy for all Europeans Package, which included various legislative measures such as directives and regulations and served an important piece of legislation since it was the first to include various obligations regarding the issue of cybersecurity for the electricity sector. The particular proposal was the Regulation on Risk Preparedness in the Electricity Sector and Repealing. It showcased that the EU member-states all follow different and uncoordinated risk management practices. For that reason, the draft regulation on the Internal Market for Electricity underlined the need for a network code developed on a European level to guarantee data protection and cybersecurity. The pilot version of the Network Code on Operational Security was designed by Entso-E[26] and obligates all electricity transmission operators to create probable cyberattack scenarios in order to create and evaluate their means of prevention. This is also complementary to the already existing legal process of the EU, namely the Network and Information Security Directive (NIS Directive), which was adopted on the 6th of June 2016.

The NIS Directive dictates the common security bases for information systems and has a special focus on "operators of essential services", which include all actors at a European level whose activities expand to numerous member states. The latter refer to: a) *suppliers of electricity and gas*, b) *refineries and processing plants*, c) *electricity and gas transmission operators*, d) *operators in the electricity and gas markets*, e) *operators of gas and oil pipelines and storage (including LNG)* and last but not least f) *gas and oil producers*. The NIS Directive also requires the development of national cybersecurity strategies by all member states. Action plans need constant adaptation to new technologies and phenomena. It also asks all EU member states to establish a Computer Emergency Response Team (CERT) as well as critical operators to notify national authorities about any possible incidents occurring. Later on, the EU plans to

[26] Entso-E is the European association for the cooperation of transmission system operators for electricity (Entso-E).

strengthen the cooperation between member states by creating and establishing a network including all national CERTs of the EU member states and has the goal to establish a strong environment of detailed information sharing. The EU plans alongside this network, to create a second one that would connect the national institutions with the European Commission. These steps are all meant to create a common EU culture on cybersecurity; something that regarding the difficulties in harmonization of the EU members states, would be difficult to achieve (Desarnaud, G., 2017). The European Union Agency for Cybersecurity (ENISA) tries to promote the cooperation of the energy community and the Computer Security Incident Response Teams (CSIRTs). It provides a Report on Cyber Security Information Sharing in the Energy Sector that firstly shares information about the development of CSIRTs, Information Sharing and Analysis Centers (ISACs) and other pertinent initiatives revolving around information sharing of cybersecurity incidents in the energy sector and secondarily aids in identifying recurrent shortcomings and issues as well as in finding good practices to address them and offering recommendations for their resolution (ENISA, n.d.)

More practically, in 2019, the European Commission proposed the Recommendation 2019/553 on cybersecurity in the energy sector as well as issued the Electricity Regulation 2019/943. The latter, in its Article 59 (2) gives the Commission the authorization to adopt delegated acts complementing this Regulation and more particularly in Article 59 (2)'s sub-paragraph e, it foresees sector-specific rules for cybersecurity issues of cross-border electricity flows, regarding planning, monitoring, reporting, crisis management as well as the minimum requirements. Moreover, the Commission Implementing Decision 2020/1479 has created a priority list regarding the network codes and guidelines for electricity from 2020 until 2023. On cybersecurity, more specifically, its Article 1, focuses on cybersecurity aspects of cross-border electricity flows (Kollau M., 2021).

Last but not least, in December 2020, the EU officials are negotiating about the drafting of a bill, that would aim to increase the cybersecurity requirements on critical companies like energy and electricity suppliers. That bill, if approved, would end up replacing the 2018 NIS Directive that introduced cybersecurity rules for critical infrastructure (Stupp C., 2021).

On an international level, the European Commission has created a working group which is working in coordination with the United States, aiming to analyse and spread good practices. The EU has also tried to create similar cooperation practices with China as well, but with no similar luck since the latter thinks that the formulation of European norms would create import obstacles for its goods (Desarnaud, G., 2017).

5.2.3. The North Atlantic Treaty Organization (NATO)

As far as NATO is concerned, the Stuxnet cyberattack, made it realize that it is important for all Allies to protect their critical infrastructure from cyberthreats, since the Stuxnet attack highlighted the vulnerability of computer networks and systems as well as the financial, structural and operational implications a similar malware could cause (Amies N., 2010). NATO has since then been strongly focusing on energy security with the Bucharest report serving as the backbone guideline for NATO's role in energy security. In addition to this, the 2010 Strategic Concept has offered NATO a cohesive narrative on energy security and its role is mainly focused in three areas. The first one is raising awareness regarding intelligence-sharing on energy development as well as political cooperation between Allies and between Allies and partners. Secondarily, the supporting of protection of critical infrastructure. Which would be possible with sharing best practices among experts alongside the organization of training courses and the insertion of energy-related scenarios in its exercises. Its last role is the enhancement of energy efficiency in the military. NATO has also created working-level contacts with the International Energy Agency (IEA) as well as will the Directorate-General for Energy of the European Commission, while the authorization of the NATO Energy Security Centre of Excellence in 2012 is also a strong and valuable player in NATO's energy security agenda.

But even though NATO has long now been focusing on energy security, it is only lately that it started focusing on energy cybersecurity due to the acceleration of cyberattacks in critical infrastructure. Even though the protection of critical infrastructure is a national level responsibility, NATO has been focusing on creating educational and training establishments for its allies to tackle the arising cyberspace challenges (Grubliauskas J., and Rühle M., 2018). Joe Biden, the current president of the United

States has stressed as part of his agenda that NATO should focus on cybersecurity on critical infrastructure. As part of this agenda, NATO will require the creation and implementation of resilient cybersecurity architectures for key critical infrastructure for both itself and all of its Allies. Such thing would require an integrated set of cybersecurity capabilities. Even though NATO cannot develop such architecture on its own, it can at the same time ask its members to do so by using the NATO Planning Process (NDPP), support a comprehensive research and show a development effort (Kramer F.D., Speranza L., and Rodihan C., 2020). Last but not least, it is important to note that the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) has signed a Memorandum of Understanding with Siemens Smart Infrastructure in order to cooperate on cybersecurity for critical infrastructure especially under CCDCEO's annual cyber defense exercise, Locked Shields[27]. With this agreement for cooperation the two parties can advance on cybersecurity for power grids (Volkwyn C., 2020).

If we take these three cases into consideration, it's fairly easy to pinpoint one main difference; the difference in policy measures adopted by a government – here the United States – and a union/ alliance – here the EU and NATO –. The United States as one government has been able to implement more quickly and more thoroughly cybersecurity measures and policies in order to protect its critical infrastructure and more particularly its energy sector from cyberattacks. In contrast, both the EU and NATO, couldn't be as quick and cannot be as strict and thorough with their measures because in these two cases we deal with a union/ alliance of different governments and different national security strategies; making it hard to create unilateral cybersecurity policies for all governments to abide by or constitutional bodies with more power.

6. Conclusions

Energy security has been a prevailing issue since the previous century, with the two oil crises of the 70s showcasing that it is of imperative need. Cyberspace is an ever-

[27] Locked Shields is a yearly exercise, organized by CCDCOE since 2010, that aids cybersecurity experts to strengthen their skills in defending critical infrastructure in real-time attacks. During the exercise, real scenarios are used with a focus on cutting-edge technologies in a simulation of the whole complexity of a cyber incident, involving strategic decision making, legal as well as communication aspects (CCDCOE).

growing domain in the 21st century, due to the ongoing great technological evolution. Moreover, energy systems are experiencing important digital changes and it is hard to know or even imagine where this could all lead. Alongside heavy and old infrastructures all interconnected components are revolutionizing energy professions. But alongside that they are also bringing a fair number of risks, which the energy industry already struggles to deal with (Desarnaud, G., 2017). Every network and computer system are interconnected and therefore, the notion that energy critical infrastructure are completely air-gapped and isolated networks and consequently unattainable is nothing but just wishful thinking.

The Stuxnet cyberattack proved that first and paved the way for more to come. Consequently, it is safe to assume that cybersecurity of critical energy infrastructure is of great importance for the safety of the energy sector. This is the reason why a lot of governments and union's such as the EU and NATO have been taking cybersecurity into consideration for many years now, but the speed of digitalization as well as of new technologies is making it difficult and more so impossible to keep up., even though constant effort is being made. As a lot of experts say, even though there is a lot of risk that has been managed to be detected, analyzed and therefore contained, a lot of risks still remain undetectable making complete protection from cyberattacks almost impossible (Desarnaud, G., 2017). This is the reason why intensive and continuous training is needed in order for constant updates being made and new protective measures being added to the arsenal of cybersecurity measures in the energy sector. Because cyberspace is a battlefield where we have to fight against an unknown, "invisible" adversary, so the only thing we can do is multiplying and upgrading our "weapons" against them as well as training ourself to be able to successfully prevent them most of the times.

7. References

1. Allan, M. (2019, October 3). *A Beginners Guide To Legacy Systems*. GoodCore. Retrieved February 26, 2022, from https://www.goodcore.co.uk/blog/legacy-systems/

2. Amies, N. (2010, October 14). *NATO includes threat of cyber attack in new strategic concept document.* Deutsche Welle. Retrieved February 26, 2022, from https://www.dw.com/en/nato-includes-threat-of-cyber-attack-in-new-strategic-concept-document/a-6072197

3. Asghar, Z. (2008). Energy-GDP Relationship: A Casual Analysis for the five Countries of South Asia. *Applied Econometrics and International Development, 8*(1), 1.

4. Assante, M. (2016, January 6). *Confirmation of a Coordinated Attack on the Ukrainian Power Grid*. SANS Institute. Retrieved February 26, 2022, from https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/

5. Boudreaux, B., and Romanosky S. (2019). Working Paper: "Private Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government." RAND Corporation.

6. Cardenas, A. A., and Safavi-Naini, R. (2012). Security and Privacy in the Smart Grid. In S.K. Das, K. Kant, and N. Zhang (Eds.) *Handbook on Securing Cyber-Physical Critical Infrastructure.* Amsterdam, Netherlands: Elsevier.

7. CCDCEO. (n.d.). *Locked Shields*. CCDCOE. Retrieved February 26, 2022, from https://ccdcoe.org/exercises/locked-shields/

8. CCDCOE. (n.d.). *Shamoon (2012)*. Retrieved February 26, 2022, from https://cyberlaw.ccdcoe.org/wiki/Shamoon_(2012)

9. CFR. (2012, August). *Compromise of Saudi Aramco and RasGas*. Retrieved February 26, 2022, from https://www.cfr.org/cyber-operations/compromise-saudi-aramco-and-rasgas

10. Cherp, A., & Jewell, J. (2014). The concept of energy security: Beyond the four As. *Energy Policy*, *75*, 415–421.

11. Collins, S., & McCombie, S. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*, *7*(1), 80–91.

12. CSS. (2017, October). *Hotspot Analysis: Stuxnet*. ETH Zürich.

13. *Cybercriminals.* (n.d.). TrendMicro. Retrieved February 26, 2022, from https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals

14. Cybersecurity and Infrastructure Security Agency. (2021, September 7). *Protecting Critical Infrastructure*. Retrieved February 26, 2022, from https://www.cisa.gov/protecting-critical-infrastructure

15. Cybersecurity and Infrastructure Security Agency. (n.d.). *About CISA*. Retrieved February 26, 2022, from https://www.cisa.gov/about-cisa

16. Desarnaud, G. (2017, January). *Cyber Attacks and Energy Infrastructures: Anticipating Risks.* Ifri Center for Energy.

17. Downey, L. (2020, November 20). *1979 Energy Crisis*. Investopedia. Retrieved February 26, 2022, from https://www.investopedia.com/terms/1/1979-energy-crisis.asp

18. Energy Expert Cyber Security Platform. (2017, February*). Cyber Security in the Energy Sector.*

19. ENISA. (n.d.-a). *Cooperation between CSIRTs and energy community*. Retrieved March 16, 2022, from https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/energy

20. ENISA. (n.d.-b). *ICS SCADA*. Retrieved February 26, 2022, from https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada

21. ENISA. (n.d.-c). *Malware.* Retrieved February 26, 2022, from https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware

22. ENTSO-E. (n.d.). *About Us.* Retrieved February 26, 2022, from https://www.entsoe.eu/

23. EUROPOL. (2018). *Internet Organized Crime Threat Assessment*. https://www.europol.europa.eu/cms/sites/default/files/documents/iocta2018.pdf

24. Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival: Global Politics and Strategy, 53*(1), 23–40.

25. Finite State. (2021). *Supply Chain Security Guidance.*

26. Flowers, A., & Zeadally, S. (2014). US Policy on Active Cyber Defense. *Homeland Security & Emergency Management, 11*(2), 289–308.

27. Fowler, K. (2016). *Data Breach Preparation and Response*. Elsevier.

28. Frankenfield, J. (2020, October 18). *Deep Web*. Investopedia. Retrieved February 26, 2022, from https://www.investopedia.com/terms/d/deep-web.asp

29. Grubliauskas, J., & Rühle, M. (2018, July 26). *Energy Security: a critical concern for Allies and partners*. NATO Review. Retrieved February 26, 2022, from https://www.nato.int/docu/review/articles/2018/07/26/energy-security-a-critical-concern-for-allies-and-partners/index.html

30. *How cyber attacks work*. (2015, October 14). National Cyber Security Centre. Retrieved February 26, 2022, from https://www.ncsc.gov.uk/information/how-cyber-attacks-work

31. IEA (2017), *Digitalisation and Energy*, IEA, Paris https://www.iea.org/reports/digitalisation-and-energy

32. IISS. (2011). Stuxnet: targeting Iran's nuclear programme. *Strategic Comments, 17*(2), 1–3.

33. Imeson, M. (2017, November 8). *Electricity industry on alert for "cyber sabotage."* Financial Times. Retrieved February 26, 2022, from https://www.ft.com/content/1fc89bd8-996c-11e7-8c5c-c8d8fa6961bb

34. *Information and Communication Technologies (ICT)*. (n.d.). Food and Agriculture Organization of the United Nations. Retrieved February 26, 2022, from http://aims.fao.org/information-and-communication-technologies-ict

35. International Group of Experts. (2017). *Tallinn Manual 2.0 on the International Law Applicable to CyberOperations* (M. N. Schmitt, Ed.). Cambridge University Press.

36. *Intranet.* (n.d.). TechTerms. Retrieved February 26, 2022, from https://techterms.com/definition/intranet

37. *IT Definition.* (n.d.). TechTerms. Retrieved February 26, 2022, from https://techterms.com/definition/it

38. Jin, X., et al. (2012). Game Theory for Infrastructure Security: The Power of Intent-Based Adversary Models. In S.K. Das, K. Kant, and N. Zhang (Eds.) *Handbook on Securing Cyber-Physical Critical Infrastructure.* Amsterdam, Netherlands: Elsevier.

39. Kollau, M. (2021, June 1). *Cybersecurity Day in the Energy Community* [Slides]. Energy Community. https://www.energy-community.org

40. Kramer, F. D., Speranza, L., & Rodihan, C. (2020, December 9). *NATO needs continuous response in cyberspace*. Atlantic Council. Retrieved February 26, 2022, from https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/

41. Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. D. Kramer, S. H. Starr, and L. K. Wentz (Eds.) *Cyberpower and National Security*. Washington, D.C.: Potomac Books.

42. Lendvay, R. L. (2016, March). *Shadows of Stuxnet: Recommendations for U.S. Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack.*

43. Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies, 22*(3), 365–404.

44. Macalister, T. (2011, March 3*). Background: What caused the 1970s oil price shock?* The Guardian. Retrieved February 26, 2022, from https://www.theguardian.com/environment/2011/mar/03/1970s-oil-price-shock

45. Malik, J. K., & Choudhury, S. (2019). Cyber Space - Evolution and Growth. *East African Scholars Journal of Education, Humanities and Literature, 2*(3).

46. Mid-Atlantic Controls. (2020, November 10). *Proprietary vs. Non-Proprietary Building Automation Systems.* MACC. Retrieved February 26, 2022, from

https://info.midatlanticcontrols.com/blog/proprietary-vs-non-proprietary-building-automation-systems

47. Mortera-Martinez, C. (2018, July). *Game Over? Europe's Cyber Problem.* Centre for European Reform. https://www.cer.eu/sites/default/files/cover_pbrief_game_over2_9.7.18.pdf

48. Nakashima, E., & Warrick, J. (2012, June 2). *Stuxnet was work of U.S. and Israeli experts, officials say*. The Washington Post. Retrieved February 26, 2022, from https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

49. Naraine, R. (2011, November 15). *Duqu FAQ*. SecureList. Retrieved February 26, 2022, from https://securelist.com/duqu-faq-33/32463/

50. Nye, J. S. (2010). Cyber Power. *Belfer Center for Science and International Affairs.* Harvard Kennedy School.

51. Office of Cybersecurity, Energy Security, and Emergency Response. (n.d.-a). *About Us.* Retrieved February 26, 2022, from https://www.energy.gov/ceser/about-us

52. Office of Cybersecurity, Energy Security, and Emergency Response. (n.d.-b). *Cybersecurity Research, Development, and Demonstration (RD&D) for Energy Delivery Systems*. Retrieved February 26, 2022, from https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

53. Paganini, P. (2016, January 12). *BlackEnergy Used as a Cyber Weapon Against Ukrainian Critical Infrastructure*. InfoSec. Retrieved February 26, 2022, from

https://resources.infosecinstitute.com/topic/blackenergy-used-as-a-cyber-weapon-against-ukrainian-critical-infrastructure/

54. Samuel, A. W. (2004, September). *Hacktivism and the Future of Political Participation.* Harvard University. https://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf

55. *Script kiddie*. (n.d.). Kaspersky IT Encyclopedia. Retrieved February 26, 2022, from https://encyclopedia.kaspersky.com/glossary/script-kiddie/

56. Shackelford, S. J., et al. (2017). From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do about It. *Nebraska Law Review, 96*(2).

57. Statista. (n.d.). *Industries impacted by cyber attacks worldwide as of September 2017*. Retrieved March 16, 2022, from https://www.statista.com/statistics/784590/cyber-attacks-on-industries-worldwide-2017/

58. Stupp, C. (2021, June 8). *European Energy Sector Prepares for New Cybersecurity Rules*. The Wall Street Journal. Retrieved February 26, 2022, from https://www.wsj.com/articles/european-energy-sector-prepares-for-new-cybersecurity-rules-11623144602

59. Styczynski, J., & Beach-Westmoreland, N. (2019). *When the Lights Went out.* BoozAllen.

60. Teplinsky, M. J. (2013). Fiddling on the Roof: Recent Developments in Cybersecurity. *American University Business Law Review, 2*(2).

61. The Editors of Encyclopaedia Britannica. (2022, January 31). *Islamic Revolutionary Corps*. Britannica. Retrieved February 26, 2022, from https://www.britannica.com/topic/Islamic-Revolutionary-Guard-Corps

62. The Editors of Encyclopaedia Britannica. (n.d.). *rootkit*. Britannica. Retrieved February 26, 2022, from https://www.britannica.com/technology/rootkit

63. The Editors of Encyclopaedia Britannica. (n.d.). *Yom Kippur War*. Britannica. Retrieved February 26, 2022, from https://www.britannica.com/event/Yom-Kippur-War

64. Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, *17*(2).

65. *turnkey system*. (n.d.). Collins Dictionary. Retrieved February 26, 2022, from https://www.collinsdictionary.com/dictionary/english/turnkey-system

66. U.S. Cyber Command. (n.d.). *Our History*. Retrieved February 26, 2022, from https://www.cybercom.mil/About/History/

67. U.S. Government Accountability Office. (2006, November 15). *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics.* Retrieved February 26, 2022, from https://www.gao.gov/products/gao-07-39#:~:text=by%20Sectors'%20Characteristics-,Critical%20Infrastructure%20Protection%3A%20Progress%20Coordinating%20Government%20and%20Private,Efforts%20Varies%20by%20Sectors'%20Characteristics&text=Because%20about%2085%20percent%20of,together%20to%20protect%20these%20assets.

68. Volkwyn, C. (2020, July 6). *Siemens and NATO CCDCOE cooperation: cybersecurity for critical infrastructure*. Smart Energy International. Retrieved February 26, 2022, from https://www.smart-energy.com/digitalisation/cybersecurity/siemens-and-nato-ccdcoe-cooperation-cybersecurity-for-critical-infrastructure/

69. Weber, J. K. (n.d.). *virtual sit-in*. Encyclopaedia Britannica. Retrieved February 26, 2022, from https://www.britannica.com/topic/virtual-sit-in

70. *What Is a LAN?* (n.d.). CISCO. Retrieved February 26, 2022, from https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html

71. *What is Low Enriched Uranium (LEU) and how it is stored at the IAEA LEU Bank?* (n.d.). IAEA. Retrieved February 26, 2022, from https://www.iaea.org/topics/leubank/what-is-leu#:~:text=Low%20Enriched%20Uranium%20(LEU)%20is,material%20to%20fabricate%20nuclear%20fuel.&text=LEU%20is%20made%20by%20enriching,is%20used%20to%20generate%20electricity

72. Whyte, C., & Mazanec, B. (2019). *Understanding Cyber-Warfare: Politics, Policy and Strategy*. Routledge.

73. Zetter, K. (2012, May 28). *Meet "Flame," The Massive Spy Malware Infiltrating Iranian Computers*. Wired. Retrieved February 26, 2022, from https://www.wired.com/2012/05/flame/

74. Zetter, K. (2016, July 6). *Hacker Lexicon: What Are CNE and CNA?* Wired. Retrieved February 26, 2022, from https://www.wired.com/2016/07/hacker-lexicon-cne-cna/

75. Φρυδάς, Ν. Π. (2018). Ο Κυβερνοχώρος και η Ασφάλεια του. Σε Μ. Σπυριδάκης, Η. Κουτσούκου, και Α. Μαρινοπούλου (Επιμ.) *Κοινωνία του Κυβερνοχώρου* (σελ. 53). Αθήνα: Εκδόσεις Ι. Σιδέρης.