American Research Journal of Humanities Social Science (ARJHSS)
E-ISSN: 2378-702X
Volume-04, Issue-07, pp-90-96
www.arjhss.com

Research Paper Open Access

Cybersecurity threats and vulnerabilities of critical infrastructures

Vlad Daniel Savin [1], Raluca Năstase Anysz [2]
[1](The Bucharest University of Economic Studies, Romania)
[2](The Bucharest University of Economic Studies, Romania)

ABSTRACT: *National electricity grids and their respective system operators play a critical role in the modernisation and digitisation of our societies. The ongoing transition to smarter grids and demand response systems, the integration of new technologies and also new consumer behaviours, as well as other challenges such as the need to improve efficiency and connect to more intermittent types of generation are all part of a plethora of opportunities which also embed a large variety of new vulnerabilities and risks. In particular, with most systems being in the digital world, this exponentially increases the risks of cyberattacks, putting at risk entire systems of smart grids and creating new challenges for the national grid to manage these threats as it moves to a more system operation-focused entity from previously a more static, distribution-focused role. This calls for the need to improve or create new defence strategies, capabilities and mechanisms. This paper first identifies the most exploited vulnerabilities in the software, hardware and network layers of national electricity grids. It then explores the threats these systems are exposed to, based on their respective vulnerabilities. Finally, it aims to offer a view of the most efficient current defence solutions - as well as a glimpse into the need for the development of new protective solutions and mechanisms.*

Keywords *–cybersecurity; industrial control systems; smart grids; malware*

I. INTRODUCTION

The economics of the ongoing Fourth Industrial Revolution force companies to adapt by incorporating new technologies and big-data-driven IT solutions. As more operations move into the digital world, cybersecurity becomes a priority for companies during this period of unprecedented change. Given the levels of complexity and ramification of digitalisation, cybersecurity becomes part of everyone's job. The hazards are inseminated via new forms of viruses and malwares. These and other aspects are at the centre of an enlarging cyber-criminal economy that is highly complicated to defence against. The World Economic Forum highlighted that cyberattacks are one of the top five international risks (Brende, 2020), with estimated damages of $6 trillion in 2021 (Walker, 2019), if defence solutions do not evolve with the speed of the technological development. The relative speed at which each move – cybersecurity defence tools vs new forms of malware – will dictate who wins and who loses. As malwares develop fast and threats become more sophisticated, defence solutions need to be a step ahead and the cybersecurity protection mechanisms need to become more complex themselves.

The national electricity grids face some of the most critical challenges as mentioned by President Trump (Winder, 2020). A power outage generated by a successful cyberattack, in its chain reaction, has the power to bring large scale disruptive impacts, not only to the powered equipment in residential homes but also to the outside world, to the national critical infrastructures like lighting, water providers, national health services and to the whole business environment, all would be left in the dark. Beyond power outages, connecting more smart appliances, with their respective demand response systems, intelligent cars and other new technologies to the grid exposes the national electricity grid and the system operator to a wider array of safety and privacy-related risks.

National distribution grids, as critical infrastructures, have sustained and provided energy for decades. The integrated and almost closed architecture has factually brought efficiencies in equipment and operations. However, beyond the distribution function, national grids have been developing more and more their system operator role. The role has primarily been to balance the electricity markets' demands, but national grids – as well as distribution grids in some regions and countries – are playing an increasingly important part also in the

integration of smarter technologies and solutions (micro-grids, batteries and demand-response systems). These come as digital operational solutions, and with that, they present new cyber vulnerabilities to the system.

As the grid expands its role and reach to respond to fresh demands on infrastructure from economic agents and customers, its protection tools need to be compatible with its new digitalised architecture. (Obodoeze et al., 2018).

New ambitions, driven either by businesses or by governments – such as climate-neutral targets, may require even further integration between smart energy systems – the national electricity grid may have, for instance, to communicate more and better with the gas grid and its supply sources, to ensure more flexibility for the take up of renewables. Building more connections between different systems in a digital manner means also, there will be a greater need to secure these connections and to identify potential vulnerabilities and threats before malwares attack these assets.

Operational Technology (OT) needs to integrate with Information Technology (IT) to drive digitalisation, automation, efficiency gains and indeed for systems to be able to deliver the new flexible solutions that consumers, businesses and governments are asking for – such as more electricity and gas systems integration, better visibility and balancing between national grids and micro, smarter grids (Ginter, 2018).

Whilst OT is a very secure, solid, tested-and-tried system – and hence harder to attack and hack, IT is a lot more permeable to cyber vulnerabilities and threats. Integrating OT with IT means not only the creation of more connectivity - it needs to involve also the creation of new security and defence systems. Only by respecting this, a full integration between OT and IT can be achieved. The challenge is a completely new one – OT was conceived initially to solve an operational problem, to act as an isolated system, it did not need sophisticated protection systems. IT brings a new dimension to these operational solutions – an opportunity to make the system more efficient and a fresh threat to its safe operation – in the form of cyberattacks.

As the barriers between Information Technology (IT) and Operations Technology (OT) disappear, Industrial Control Systems (ICS) environments are increasingly exposed to an increasing volume and complexity of cyberattacks (Alexander, 2013). Recently, cyberattacks have been very aggressive on industrial control systems. These have included the development of new malwares to take advantage of identified vulnerabilities, as well as Advanced Persistent Threats driven by national interests (Jang-Jaccard et al., 2013). At the same time, counter-espionage services, along with organized groups driven by internal and external interests - and often financially motivated - have started to engage in terrorist cyberattacks targeting critical infrastructures such as industrial networks, especially the networks of national electricity grids. Given the extensive development on the integration of the OT with IT systems, the volume of cyberattacks can only intensify in time, possibly disturbing the operations of the Industrial Control Systems (Potlapally, 2011).

Several ICS studies have been reviewed for the purpose of this paper, to identify current, as well as emerging cybersecurity threats and vulnerabilities. The consensus is that ICSs have evolved from an isolated type of platform to an open one, which is highly vulnerable to the expanding IT vulnerabilities and threats. In 1997, Kaspersky, an antivirus software developer, discovered just two cyber vulnerabilities (ICS, 2019). In 2010, the number increased to 19. After another 5 years, in 2015, the number of vulnerabilities multiplied by 10, to 189, which shows the amount of interest the domain receives from the different stakeholders.

The changing technological environment brought by the Fourth Industrial Revolution creates the need for technological systems to monitor and control ICSs. These were previously isolated types of infrastructure. However, with more communication channels between the infrastructure capabilities – with monitoring and controlling now more linked together, the risks of the new cyber vectors like malware, phishing, ransomware, DDoS or Zero-day exploits also increases.

Cyber operating systems are here and will only expand in time. With them, cyber challenges will also develop and enlarge, and there is no single silver bullet to address them – challenges are operation-system-specific, and they change as rapidly as or more than the systems themselves. The attention that is given to such topics needs to reflect the risks posed by the expansion of systems in the cyber space. The fact that many businesses have been built on singular, isolated OT systems means the practice of giving enhanced attention to cyber-security issues has not developed as thoroughly as the new technological wave would need it to. Understanding the risk and preventing it has to be entrenched in the building out of smarter, cyber-systems. The cyberattacks will bring new responsibilities for those in charge of security. The critical industrial infrastructures are experiencing alterations to become “smart”. In contrast to traditional systems, a smart system enables the grid to incorporate new technologies and resources. By adopting new emerging data transfer systems that allow information flows between the grid and its different external stakeholders, the grid will become more exposed to cyberattacks. The advantages of the smart grid with its technological tools are clear, but the modernisation process will not be a straightforward one. The modernisation will probably happen in stages, the full process probably will be at least a decade lasting one. There will be challenges and vulnerabilities for the ICSs operators during the transition process because the new systems will interfere with the existing ones and probably other ICSs plant operators will be at different stages in their OT and IT integration – this will only further increase the

complexity of the upgrade process. Meanwhile, when an ICS cannot be shut down during the upgrade process, the associated risks increase.

In order to understand the cyberattacks threat vectors, this paper analyses the most commonly exploited vulnerabilities in existing ICS software, hardware and network layers, as well as analyses the proposed defence methods against such exploitations.

Figure 1. Summary the focus of the paper

	Hardware	Software	Network
Common threat	Trojan Hardware	Program bugs	Protocol attacks
	Clones	Design bugs	Monitoring and sniffing
	Side channel attacks	Errors in deployment	
Defense mechanism	Hardware that is tamper resistant	Secure coding practice	Firewall
	Hardware watermarking	Secure design and development	Intrusion detection systems
		Formal methods	VPN
			Encryption

II. SOFTWARE VULNERABILITIES

Program errors create software vulnerabilities. A software fault is the common indication used to define a deficiency in a computer program. Cyberattacks usually use software imperfections such as design flows, missing data encryption, SQL injection, buffer overflows, issues with libraries and other type of bugs in order to control the systems in unintended ways from the original design, thus obtaining unauthorised access to data, compromising it or causing Denial of Service (DoS). The majority of cyberattacks continue to use system bugs and design flows – making these the key vulnerabilities in information security. Programming errors can open the door for attackers even in front of Firewalls, Intrusion Detection Systems (IDS) or other defence protocols. Thus, it is imperative to prevent, detect and react to the software imperfections. In this section, the paper describes the main software vulnerabilities.

- **Types of Software Vulnerabilities**

o **Buffer Overflow**

Software exploitation happens when a software is abused. The majority of cyberattacks target software vulnerabilities by taking advantage of snags in memory, user validation and access privileges (Howard et al., 2005). The attack on memory safety is executed by modifying the contents of memory. One of the common ways of achieving is by buffer overflow. The attack on buffer overflow happens when a program stores more information in a buffer than it was built to hold. Since the buffer is programmed to keep a certain amount of data, the extra information can overflow and corrupt by overwriting valid data in other adjacent buffers.

o **Data Validation**

The process of input validation refers to the process of data flowing in a certain way. Misleading data validation can drive data to corrupt SQL databases. SQL injection is one of the most common attacks into a website's database. An attacker inserts SQL commands to alter the database. The attacker exploits a defect knowing that the output is reliant on the successful application of other successive events.

o **Other Types**

Race condition error is the attack that causes changes in system between the checking of a condition and the usage of the outcomes of that check.

Privilege confusion is another attack exploit by getting access to information that is normally protected. The result is that attackers gain access to confidential data.

- Existing Defence Software Solutions

The attempts to solve these software vulnerabilities can be grouped in:

a) Detection of malicious code;

b) Detection of programming flaws, errors and patch releases to solve flaws;

c) Sandboxing.

The primary objective for all is to develop solutions and to create a safe programming environment and context. Engineers look and discover the common errors that lead to software threats and vulnerabilities and try to establish a better-secured software code.

- **IDS and anti-malware**

IDS and antivirus software are the most common tools for detecting attacks. IDS detect exploits or interactive attackers while antivirus scanners detect malware. Antivirus scanners are the most popular defence mechanisms. They detect known codes of malware (signatures).

- **Type-safe programming languages**

Secure design and development is a technique that verifies that the program is defect-free. The testing software errors is a tool developed to uncover flaws in programming languages. The testing software module was designed to check and ensure that the application performs as expected, meets the security requirements and does not contain errors or bugs. The testing process consists on trying to identify defects, which are considered variances between the actual and the expected results. A type-safe language program also prevents memory management errors. Reducing programming errors aims to limit the privileges a program has while running. The mechanism follows the principle of least privilege - an old design principle. The main idea is to offer the program only the rights needed to operate. By limiting these privileges, the possible damages are restricted in case of an attack.

- **Sandboxing**

Another emerging cyber defence tool is sandboxing, which executes and verifies the code in a restricted virtual environment, limiting the initial access to the operating system, before granting the access of the code to be executed on the physical system.

III. HARDWARE VULNERABILITIES

Hardware components represent the physical parts of a computer. Through exploitation of the hardware vulnerabilities, attackers can make use of known weaknesses to control the system (Constantin, 2020). In comparison with software-level attacks where updates, patches, newly developed detection tools for intrusion and antivirus programs search to identify malware, the majority of the hardware-based cyberattacks are susceptible to escape such detections. Taking advantage of these deficiencies, hardware-based attacks targeting the weaknesses are on the rise (Potlapally, 2011).

- **Types of Hardware Vulnerabilities**
  - **Trojans**

Trojans for hardware equipment are the most common hardware malwares. A hardware Trojan maliciously modifies the logic behind the electronic circuits in order to alter the planned process of the system. They have a variety of troublesome effects. A hardware Trojan might change, when triggered, an electronic circuit to provide remote unauthorised permission or to accept commands that otherwise should be rejected. Another type of Trojan might attach the chip's buffets and hence consume more power than normal. In a more serious scenario, Trojans might prevent operations of a resource. A DoS Trojan could affect the target module to exhaust its scarce resources. It could also physically affect the device's settings, including to ignore commands from other peripherals or simply to destroy the components.

  - **Illegitimate Hardware Copies**

Illegitimate copies of hardware are another main source of malicious exploitation since they can contain Trojans. The pressures of the current economic context to reduce costs has increased the trend for companies to purchase untrusted hardware from cheaper sources. The current economic model forces outsourcing and buying tampered-off equipment from untrusted factories in low-cost countries. Furthermore, businesses driven by the need of reducing costs may purchase untrusted hardware such as Firewalls and Access Points from untrusted online marketplaces, which do not have any guarantee of being free of malicious Trojans.

These practices also raise the possibility of the intellectual property rights to be accessed by unauthorised personnel.

  - **Side Channel Attacks**

Another example of hardware exploitation is the side channel type of attack. These materialize when attackers obtain valuable insights about a system's configuration by analysing the physical details of that device including information such as power consumption.

- **Existing Security Hardware-oriented Solutions**

Different ways have been proposed to divert the attacks on hardware equipment.

  - **Tamper-resistant**

Hardware equipment that is tamper-resistant has become critical due to its position within the networks as an entry point to the network's security.

  - **Trusted Computing Base**

Another development has been the Trusted Computing Base (TCB), which is considered as the set of hardware components that are valuable to the security of the whole network. Rigorous checks are done to audit these devices to ensure the security of the TCB and thus of the entire network. These safety mechanisms are in place to divert the attackers from getting the critical design elements of the industrial systems.

- **Distortions**

Other defence measures to protect against hardware vulnerabilities through side attacks include distortions, so that information cannot be replicated thus reducing any interrelationship between data and the emission of the side channels.

IV. NETWORK ARCHITECTURE AND PROTOCOL VULNERABILITIES

When the network protocols were developed, they were designed to support entirely different environments, which were smaller in scale. Given the complexity and large dimensions of today's industrial networks, they do not properly work in these environments. The weaknesses of the protocols become more evident when the operators and users have narrow knowledge of the architecture of the networks. Examples of this limited knowledge include insufficient encryption schemes, patches not applied in time and lack of properly configured security filters and policies.

- **Types of Network Layers and Protocols vulnerabilities**

Cyberattacks commonly happen by manipulating the limitations of the following protocols: Internet Protocol (IP), Transmission Control Protocol (TCP) and Domain Name System (DNS).

- **IP**

The Internet Protocol is the main protocol on which the traffic within the network happens. It offers the main data needed for packets to route between computers and routers. However, the IP was not built to check the authenticity and privacy of the data transmitted. This embedded lack of security permitted the packets to be hijacked or changed while they were routing over unknown networks.

- **IPSec**

To solve this gap, another protocol was developed, IPSec, which provides secured and encrypted IP traffic. This protocol has been used for the establishment of the VPN, which forms a secure route between a computer from outside and a trusted network.

- **TCP**

The TCP protocol makes sure that the packets are transmitted in reliable way and directs the order in which the packets are transmitted.

- **SSL**

SSL protocol was developed to offer security between end-to-end computers.

- **DNS**

The DNS protocol uses human-readable host names and translates them into IP addresses. The DNS replies are not authenticated - a hacker can send DNS messages to imitate an Internet server. The DNS servers have been one of the common target of the DoS attacks creating important interruptions in the internet.

- **Existing Security Network and Protocol-oriented Solutions**

- **Cryptography**

Cryptography is the most common system to protect information. It aims to offer confidentiality, message integrity and authentication in an unsecured network. It is a principle tool to safeguard the information sent between users by encoding data so only users with the right keys can decrypt the information.

The emergence of new technologies has allowed attackers to have powerful exploitation tools that are used to decrypt the existing encryption algorithms. Given the dangers, the American National Institute of Standards and Technologies has changed the SHA-1 (Secure Hash Algorithm) protocol with the SHA-3, a more advanced encrypting protocol (Bryson, 2015).

Skilled attackers use refined techniques to camouflage traffic loads to look more like genuine traffic. Furthermore, big data flowing on networks requires new analysis algorithms to analyse the uncertainty of information attached. This has led to the creation a new domain of research, where network security experts collaborate with the design community to elaborate better ways for visualizing the traffic in order to understand the breaches. The resulting data is then analysed by network experts.

- **Firewalls and IDS**

Typical network defence tools include Firewalls and Intrusion Detection Systems (IDS). The Firewall is the most common tool to protect the systems within the internal network from external attacks. The way it works is by analysing the data packets and determining whether they should be allowed, based on the rules set by the network administrator.

Firewalls can be placed in many layers in the network infrastructure. Network layer Firewalls filter traffic at the edge of the network and blocks packets unless they match certain rules defined by the network administrator. The New Generation of Firewalls (NGFW) have become more sophisticated in order to keep pace with the new threats, being able to protect against more complex types of malware, like Advanced Malware Payloads (Alto, 2020).

The proxy server is similar with a Firewall by responding to the input packets and blocking depending on the policies set by the administrator. Both layering tools, firewall and proxies, make it more difficult to manipulate the internal system.

The emergence of new technology increased the capability of the attackers to create more advanced cyber malwares. The intrusion detection systems (IDS) analyse any suspicious activity over the network. These detection systems are extremely valuable that they detect attacks in early stages and then can protect further the system from subsequent attacks. In addition, these systems help detect any sign of suspicious activity generated by a user, application or a malware.

The system analyses the normal traffic by examining the pattern and reporting abnormal traffic. Such detections are either anomaly-based or signature-based. In the signature-based analysis, the system detects the malicious packets based on their signatures as they route. However, signature-based IDS have been considered ineffective as the sophistication of malware has developed – and hence, advanced anomaly-based IDSs have been designed. In anomaly-based signature analysis, the system has no expertise of how the malicious packets look like but analysis the changes in behaviour of the system, thus alerting immediately when detecting suspicious software behaviour. These systems learn with the help of Artificial Intelligence and Machine Learning technology what is supposed to be normal and legit traffic for an extended period.

Still, more holistic approaches to better protect networks are needed, instead of focusing only on configuring specific assets such as Firewalls or IDS.

Best practices identified by network-forensic studies include understanding the traffic attack patterns and locating the hackers (Ayodeji et al., 2020).

Another way is to create honeypots (Baykara and Das, 2018). A honeypot is a defence tool that mitigates cyberattacks by attracting the hackers to parts of the system that appear to contain legitimate information. Honeypots trap the attackers into them in order to understand their techniques better. All the attack information captured by the honeypots is analysed in order to improve protection against future attackers.

V. RESULTS AND DISCUSSION

The recent digitalization of the world economy, coupled with the growing penetration of the smart machines and industrial systems, has led to operating systems being increasingly exposed to cyberattacks. There is a plethora of ways to protect against such attacks, however more holistic approaches need to build on existing IT solutions. As the world continues to modernise and as it becomes more technological, cyber malware solutions need to keep the pace with all developments and continuously evolve. OT and IT have long started to become more integrated but new ambitions continue to arise. The previously more static and isolated systems belonging to the traditional architecture of most businesses, including that of large bodies like the national grid for instance, is changing as they adapt to more automation and as they increase efficiencies. This creates a wider array of safety-related and privacy-related risks. In building out the new architectures, these risks need to be accounted for, in order to be one-step ahead of malware systems. Adapting old architecture to new cyber security solutions may be burdensome or impossible. Legacy equipment, safety regulations that may prohibit any modifications being made to equipment and compliance regulations that require sensitive data to be made available to third parties are further challenges. Whilst further efficiencies and developments represent a significant gain for industries, creating new structures without their protective shell poses considerable risks.

As cybersecurity vulnerabilities and threats expand for critical infrastructures, the industry's resilience to defence against such threats also needs further development. Different techniques and tools exist to remedy vulnerabilities in software, hardware and networks; however, the consensus is that the best technique is the one that protects everything from inside out (David and Thomas, 2019). The overwhelming majority of companies protect their perimeters to guard their networks from any outside possible attack.

This research paper has focused on the cyber vulnerabilities and threats that pose risks to the modern national electricity grids. Based on the research done, it presented the main vulnerabilities facing the software, hardware and networks layers of the Industrial Control Systems and presented the existing defence solutions to address these.

The results provide administrators in charge of the ICS cybersecurity an insight into the key elements that need protection and the means to achieve such protection for the successful deployment of a holistic cyber security strategy.

However, whilst the paper discusses the existing cyber risks and defence mechanisms and solutions, significant challenges are presented by the constantly evolving and developing of cyber threats, so ICS administrators have to continuously monitor and deploy the latest defence tools to secure their assets. Further research is needed to identify threats before they emerge and hence keep a step ahead of possible attackers to best protect and fully integrate OT and IT systems within the more digitalised and ultimately more customer-responsive ICS infrastructures. Finally, emerging technologies, as they face their own new, unique cyber threats, will need fresh defensive mechanisms – for which research and investments will be needed.

VI. ACKNOWLEDGEMENTS

ACKNOWLEDGEMENTS

I would like to express my gratitude to Professor Nadia Ciocoiu, Professor Silvia Fotea and Professor Ioan Fotea for the valuable support and guidance provided.

REFERENCES

[1]. Alexander, D., 2013. Information Security Management Principles. BCS, The Chartered Institute for IT.

[2]. Alto, P., 2020. Firewall Feature Overview Datasheet [WWW Document]. Palo Alto Networks. URL https://www.paloaltonetworks.com/resources/datasheets/firewall-feature-overview-datasheet (accessed 7.31.20).

[3]. Ayodeji, A., Liu, Y., Chao, N., Yang, L., 2020. A new perspective towards the development of robust data-driven intrusion detection for industrial control systems. Nuclear Engineering and Technology. https://doi.org/10.1016/j.net.2020.05.012

[4]. Baykara, M., Das, R., 2018. A novel honeypot based security approach for real-time intrusion detection and prevention systems. Journal of Information Security and Applications 41, 103–116. https://doi.org/10.1016/j.jisa.2018.06.004

[5]. Brende, B., 2020. The Global Risks Report 2020 [WWW Document]. World Economic Forum. URL https://www.weforum.org/reports/the-global-risks-report-2020 (accessed 7.29.20).

[6]. Bryson, J., 2015. Hash Functions | CSRC [WWW Document]. NIST. URL https://csrc.nist.rip/publications/fips/fips180-4/fips-180-4.pdf (accessed 7.31.20).

[7]. Constantin, L., 2020. 32 Hardware And Firmware Vulnerabilities: A Guide To The Threats [WWW Document]. CSO Online . URL https://www.csoonline.com/article/3410046/31-hardware-and-firmware-vulnerabilities-a-guide-to-the-threats.html (accessed 7.31.20).

[8]. David, J., Thomas, C., 2019. Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic. Computers & Security 82, 284–295. https://doi.org/10.1016/j.cose.2019.01.002

[9]. Howard, M., 2009. 24 Deadly Sins of Software Security. McGraw Hill Professional, New York.

[10]. ICS, K., 2019. Threat Landscape For Industrial Automation Systems, H1 2019 | Kaspersky ICS CERT [WWW Document]. Kaspersky. URL https://ics-cert.kaspersky.com/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/ (accessed 7.31.20).

[11]. Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P., Jones, K., 2015. A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection 9, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002 Jang-Jaccard, J., Nepal, S., 2013. A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences, 80 (2014), 973-993.

[12]. Lonsdale, D.J., 2004. The nature of war in the Information Age. Psychology Press, Portland, OR.

[13]. Obodoeze, F.C., Obiokafor, I.N., Asogwa, T.C., 2018. SCADA for National Critical Infrastructures: Review of the Security Threats, Vulnerabilities and Countermeasures. IJTSRD Volume-2, 974–982. https://doi.org/10.31142/ijtsrd9556

[14]. Potlapally, N., 2011. Hardware security in practice: Challenges and opportunities. 2011 IEEE International Symposium on Hardware-Oriented Security and Trust. https://doi.org/10.1109/hst.2011.5955003

[15]. Vacca, J.R., 2013. Cyber Security and IT Infrastructure Protection. Syngress.

[16]. Walker, I., 2019. Cybercriminals Have Your Business In Their Crosshairs And Your Employees Are In Cahoots With Them [WWW Document]. URL https://www.forbes.com/sites/ivywalker/2019/01/31/cybercriminals-have-your-business-their-crosshairs-and-your-employees-are-in-cahoots-with-them/#47311ea31953 (accessed 7.29.20).

[17]. Winder, D., 2020. Trump Declares National Emergency As Foreign Hackers Threaten U.S. Power Grid [WWW Document]. Forbes. URL https://www.forbes.com/sites/daveywinder/2020/05/02/trump-declares-national-emergency-as-foreign-hackers-threaten-us-power-grid/#5876edf83497 (accessed 7.30.20).