REVIEW

Annals of Disaster Risk Sciences

Vol 3, No 1 (2020): Special issue on cyber-security of critical infrastructure

Artificial Intelligence Techniques to Prevent Cyber Attacks on Smart Grids

Fabrizio Bertone, LINKS Foundation
Francesco Lubrano, LINKS Foundation
Klodiana Goga, LINKS Foundation

Address for correspondence: Fabrizio Bertone, LINKS Foundation, Italy, e-mail: fabrizio.bertone@linksfoundation.com

Abstract

Energy is one of the main elements that allows society to maintain its living standards and continue as usual. For this reason, the energy distribution is both one of the most important and targeted by attacks Critical Infrastructure. Many of the other Critical Infrastructures rely on energy to work reliably. Some states are particularly interested in getting stealth access to -and take control of- energy production and distribution of other Nations. This way they can create huge disruption and get a significant advantage in case of conflict. In the recent past, we could observe some real-life demonstrations of this fact. The introduction of smart grids and ICT in the management of energy infrastructures has great benefits but also introduces new attack surfaces and ways for attackers to gain control. As a benefit, we can also collect more data and metrics to better understand the state of the grid. New techniques based on Artificial Intelligence and machine learning can take advantage of the available data to help the protection of the infrastructures and detect ongoing threats. Smart Meters which are connected intelligent devices spread over the grid and the geographical distribution of the population. For this reason, they can be very useful data collection assets but also a target for attack. In this paper, the authors consider and analyze various innovative techniques that can be used to enhance the security and reliability of Smart Grids.

Keywords

Smart Grid cybersecurity, Anomaly detection, Artificial intelligence protection

1. Introduction

Energy, and in particular electricity, is one of the fundamental building blocks for modern societies. According to a report from ENISA, Energy is the only sector, together with transport, that is recognized as critical by all 18 considered European States (Mattioli & Levy-Bencheton, 2014). Most other sectors, if not all, depend directly or indirectly on Energy to function on a day-to-day basis.

Energy sector is both one of the most affected by cyber-crime, and one of the most costly in all affected sectors (Tofan, NIKOLAKOPOULOS, & Darra, 2016) (Ponemon, 2019).

In the last two decades, we have seen cyber-attacks and incidents of various magnitudes of impacts on each and every sector (F-Secure, 2019) concerning energy production (Wallace & McClure, 2014), transmission and distribution. Gas (Reed, 2004) and Oil industries (Hacquebord & Pernet, 2019), utilities and even nuclear power

plants (Kesler, 2011) have been hit by targeted or untargeted attacks. Many other incidents might very likely have been kept undisclosed to the general public or not discovered at all.

More and more Advanced Persistent Threat (APT) groups, especially the ones following nation-states objectives, are becoming active and stealthily infiltrating Critical Infrastructure to steal information or just keeping a foothold inside the systems to quickly act in case of escalading warfare (e.g. to create disruption).

It is complex to efficiently identify security threats. Studies show that security breaches are in average discovered only dozen to hundreds of days after the initial intrusion, if at all. While the trends show a decreasing of the detection time in the last five years, it is still unacceptable high (FireEye , 2019). Smart Grids are complex systems and tricky to monitor. To quote the head of information security at Enel Italy: "*We have huge background noise in the identification of cyber threats. Enel's global IT security infrastructure identifies more than 100,000 events a day*" (Bundock, 2015). These numbers can be easily overwhelming and cover the real threats, especially if skilled attackers make their best to hide their traces inside the noise. Artificial Intelligence techniques could help improving the detection rates.

The document is structured as follow: section 2 briefly describes some notable recent attacks against various energy infrastructures around the world. Section3 gives an introductory overview of the Smart Grid, and its characteristics. In section 4 is performed an analysis of various Smart Grid threats, where a review of possible solutions follows each issue considered. This section also lists some commercial solutions already in the market that can enhance the security of various aspects of the Smart Grid using Artificial Intelligence techniques. Section 5 concludes the paper with final considerations and closing remarks.

2. Notable Attacks Against Energy Infrastructure

Recent years have seen a growing number of cyber-attacks targeting various infrastructures and enterprises of the energy sector. Sophisticated malware and toolkits have been developed specifically to hit just some specific systems. What follows is a non-exhaustive list of some of the most notorious and notable attacks of the past years, in order to better understand the context and the hazards surrounding the sector.

Stuxnet - Stuxnet is a malware first discovered in 2010 on an Iranian computer, and became the most notorious example of extremely sophisticated malwares targeting industrial components. It was designed to specifically sabotage centrifuges in the Iranian nuclear facility of Natanz and disrupt the uranium enrichment process. Exploiting four zero-day vulnerabilities on Windows, Stuxnet modified the parameters that limited the maximum spin speed of the nuclear centrifuges (Langner, 2013). This leaded to the destruction of about one fifth of the Iranian's nuclear centrifuges. While the main target of the malware was that specific facility, it was later identified in other energy plants.

Shamoon - Shamoon is the name given to a malware that targeted Saudi Aramco (oil, Saudi Arabia) and RasGas (natural gas, Qatar) systems in 2012 (BRONK & TIKK–RINGAS, 2013), making thousands of workstations unusable and disrupting operations. An enhanced version of the malware, called Shamoon 2.0, targeted various organizations in Saudi Arabia starting from 2016 (Kaspersky Lab, 2017). A furtherly improved version, called Shamoon 3, hit the Italian oil company Saipem in December 2018 (Blueliv, 2019).

Dragonfly/Havex - Havex is a Remote Access Trojan (RAT), a malware category that aims to control a system through a remote network connection. An espionage campaign organised by the Dragonfly group leveraged Havex malware to collect information targeting different industry sectors, among which the energy. Havex is estimated to have impacted as many as 2000 infrastructure sites, a majority of which were in Europe and the United States (Nelson, 2016).

BlackEnergy - BlackEnergy malware is a botnet that evolved over time, starting from a web-based distributed DDoS platform to a plugin architecture. One of the most relevant attack conducted with BlackEnergy was against a regional Ukrainian electricity distribution company (Lee, Assante, Conway, 2016). The malware infected the SCADA systems of the company and on the 23th December 2015 several electrical substations were disconnected for about 3 hours, leaving more than 200,000 customers without electricity during a cold winter day.

Industroyer - Industroyer, also known as CrashOverride, is one of the biggest malware threat to critical infrastructures. Like BlackEnergy malware, Industroyer has been designed to attack the ICSs used in electrical substations. The developers of Industroyer malware were people with a deep knowledge of ICS and probably an access to the specific equipment used in the targeted electricity industry. Industroyer targeted the Ukraine's power grid causing a blackout in Kiev (Dragos, 2017).

TRITON - TRITON is another example of identified malicious software developed to target safety instrumented systems (SIS). This malware consists of a python script depending on a zip file containing several libraries, among which the modified Triconex framework to interact with the Schneider Electric Triconex safety systems. The targeted systems are the ones responsible of the last line of defense of critical systems, such as petrochemical plants, water treatment facilities and nuclear plant (Dragos, 2017). TRITON is possibly the first malware designed aiming to put lives at risk.

Most of the presented attacks exploited either the Industrial Control Systems used for the automation of processes or the ICT and software components, all of them being integral part of the Smart Grid concept described in next section. A comprehensive list of cyber-attacks involving energy infrastructures is available in (ECSO, 2018).

3. Smart Grid and the Advanced Metering Infrastructure

The main focus of this paper is specifically on the Smart Grid. As a matter of fact, the traditional power generation and transmission systems were no more sufficient to cover the new requirement introduced by modern cities and societies. The new paradigm of Smart Grid, based on the availability of new information streams used to control the stability and reliability of the power supply, and to offer new enhanced services and markets (Demand-Response, Transactive Energy, etc), is implemented by the introduction of the Advanced Metering Infrastructure (AMI).

The AMI is actually the integration of ICT, ICS and IoT technologies into the legacy "dumb" power systems. A schematic overview of the components and technologies involved in a modern AMI is visible in Figure 1.

Smart grids are then the interconnection of complex systems composed by heterogeneous devices and linked together by many different types of transmission mediums and protocols.

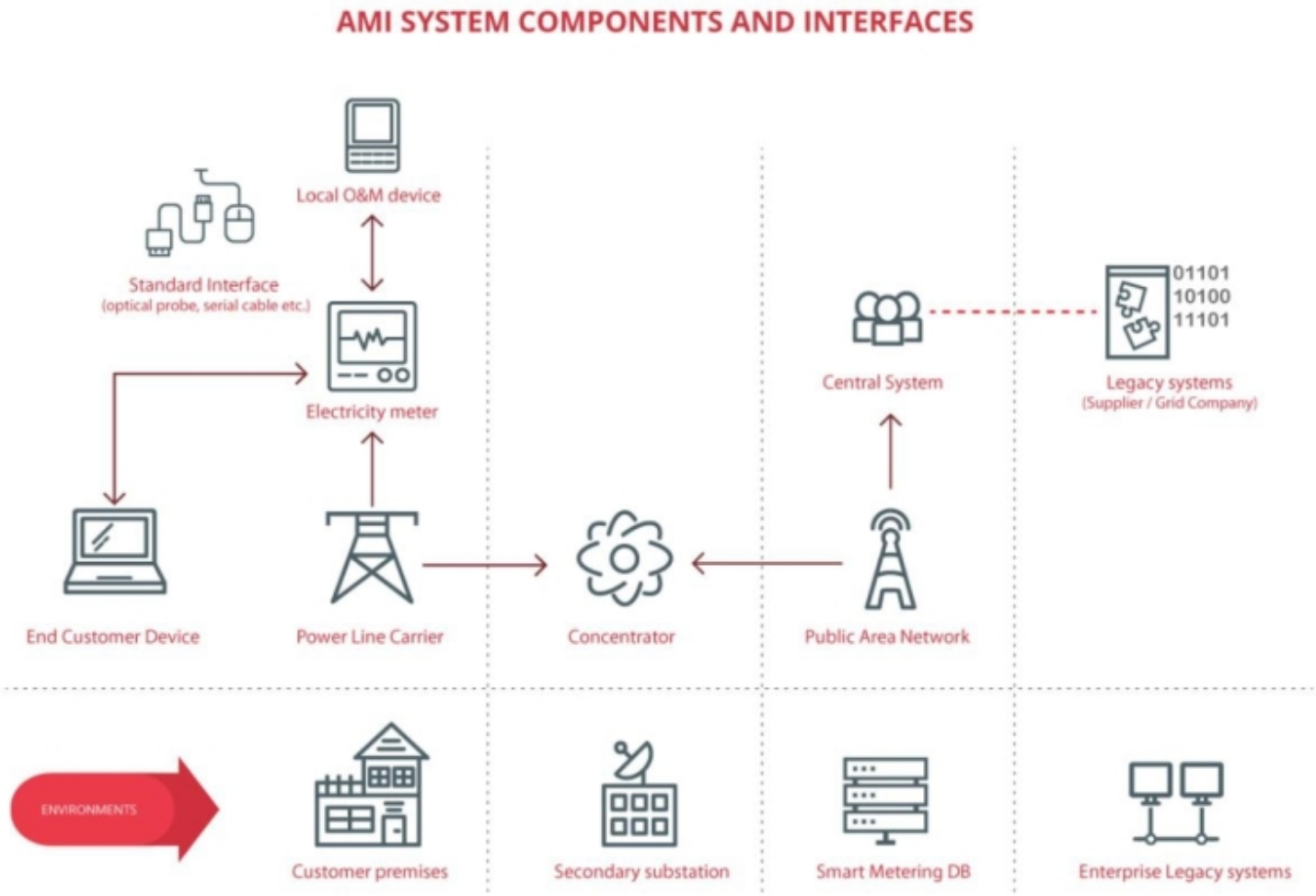

Figure 1. Main components of Advanced Measure Infrastructure (INCIBE, 2017)

While newer protocols support –but not always enforce- security mechanisms like encryption or mutual authentication, legacy protocols usually don't even support basic security (Collantes & Padilla, 2015) (INCIBE, 2017), leaving the doors open to multiple kind of attacks.

4. Threats of the Smart Grid and Defensive Techniques

The Smart Grid is made by physical components, like power generators, and digital controller and connecting assets. Given the complexity of the smart grid systems, different strategies could be used to disrupt its normal function. The actors and causes that can be source of threat for Smart Grids are multiple and of different origin. A detailed review is presented in (Otuoze, Mustafa, & Larik, 2018). (Gunduz & Das, 2018) divide attacks in two classes: passive and active attacks. Passive attacks are used to obtain information about the system configuration, architecture and behavior through eavesdropping techniques. Active attacks aim to affect the normal operations of the system. A survey of cyber-security challenges that involve Smart Grid is done in (Lopez, Sargolzaei, Santana, & Huerta, 2015). Other threats, involving more the traditional ICT components, are considered in (El Mrabet, Kaabouch, El Ghazi, & El Ghazi, 2018). Only a subset of those are considered in this paper. In particular, we consider the threats that pose serious menaces to the whole infrastructure, ignoring threats to customer's privacy, passive espionage and similar issues.

A general Artificial Intelligence concept that is applicable for the identification of malicious activities is the *Anomaly Detection*. The purpose of anomaly detection algorithms is to identify rare events, that in this context represents things like the suspicious behaviors of some user or device, unusual network traffic or similar.This methodology can be applied to single aspects of the Smart Grid at a time or using a holistic approach, that means considering the behavior of the *whole* system at a time.

An example of the latter approach is presented in (Marino, et al., 2019). Authors of that research used a simulation platform, with Hardware-in-the-Loop, to generate data describing both physical and "cyber" behaviors of a grid configuration. Using the generated data, they were able to implement machine learning algorithms able to reliably identify multiple kinds of ongoing attacks. The convenience of the technique used is that only normal behavior data is required to train the algorithms. Attacks are automatically recognized as anomalous configurations and notified. A similar methodology is also used in (Karimipour, Geris, Dehghantanha, & Leung, 2019), where unsupervisioned machine learning algorithms are implemented so that they can discriminate between a "normal" fault and a real cyber-attack.

In (Rossi, Chren, Buhnova, & Pitner, 2016), authors describe the results of analysis done on real smart grid data streams collected via distributed smart meters. The research points out that it is important to consider a *collective* and *contextual* approach to anomaly detection, while *single point* anomaly detection resulted to be useless.

4.1 Threats of the Smart Grid and Defensive Techniques

This section describes some threats that involve the physical components and limitations of the power distribution systems.

- Load Altering

The electricity distribution grid is a system bound to physics laws such as *Kirchhoff's rules,*and must respect very strict constraints in terms of maximum power flow, voltage, frequency and so on. In case of issues, appropriate reactions must be taken very quickly in order to avoid cascading effects and the disruption of the service. A distributed and coordinated altering of loads could be very harmful to the grid (Mohsenian-Rad & Leon-Garcia, 2011). The introduction of more and more pervasive IoT devices and technological Home Assistants, greatly enhance the possibility of successfully implementing this kind of attack. (Soltan, Mittal, & Poor, 2018).

While the effects of those kind of attacks could somehow be seen by the regular controlling devices as voltage or frequency alterations, this is not enough to precisely detect where the problem lies, and could not be easily detected as an attack and differentiated by "regular" unbalances. Such kind of threats could only be detected by monitoring the load of each single consumer. While smart meters could be used for this purpose, today's smart meters just keep track of energy –and not instant power- consumption in timeslots of 15 minutes or so. This is not enough to detect the presented attacks. A device to do so should have the characteristics of real-time notification of significant consumption variations, like the Event-Driven Metering presented in (Simonov, Chicco, & Zanetto, Event-driven energy metering: Principles and applications, 2017).

A solution to this kind of attack, taking advantage of the information made available by Event-Driven Meters has been proposed in (Simonov, Bertone, & Goga, Detecting the Manipulation of Demand via IoT, 2019), where the density of events is used to discriminate between regular consumptions and coordinated attacks.

- Time (de)Synchronization Against PMU

Phasors Measurement Units (PMU) are fundamental controlling devices used to assess and stabilize the frequency of the AC electricity flow. They are highly dependent to a precise synchronization of the timing between PMU deployed in different segments of the grid. To keep synchronization, GPS clock or other protocols are used. Spoofing attacks can be used to desynchronize the PMUs and force the execution of inappropriate reactions. In this case it is complicated to efficiently use AI mechanisms as the required reaction time is very limited. It is however possible to identify attacked PMU in order to increase their protection by other means. A solution that define new Time Synchronization Attacks detectors is presented in (Shereen & Dán, 2020).

- Generators and Industrial Control Systems Tampering

In current grids, electricity is commonly produced using rotational generators, that can be operated by fuel, wind, water, steam or other means. In AC networks, it is fundamental that every generating device/asset is synchronized with the frequency of the grid. This is to protect both the grid stability and the safety of the generator. If a generator

is forced to operate out of sync with respect to the frequency of the grid, it can suffer very strong mechanical stress, that can quickly lead to the destruction of the device. This has been demonstrated in a controlled environment, causing the explosion of the generator (Bernabeu & Katiraei, 2011). Moreover, this could compromise the safety of nearby operators or casual passerby posing a serious risk of injuries and could also initiate cascading effects leading to the shutdown of the grid and consequential blackout. The same technique of inducing mechanical stress to physical assets can be used (and has already been demonstrated and exploited) in other contexts. Predictive maintenance techniques based on monitoring vibrations or other environmental information could be used to detect this kind of threats (Vanraj, Goyal, Saini, Dhami, & Pabla, 2016), (Gebraeel, Lawley, Liu, & Parmeshwaran, 2004), (Durbhaka & Selvaraj, 2016).

4.2 Threats Against the AMI and Smart Meters

The development of malicious programs and potential unwanted applications is a known issue that is increasingly affecting IoT devices besides common system operators (such as Windows, MacOs, Android, etc.). The digitalization of industrial operational technology and the wide spread of IoT systems is rapidly increasing the number of connected devices. Consequently, this increase the number of targets, most of them unprotected of poorly protected against cyber-attacks (AV-TEST). One of the most relevant examples is the Mirai attack. The Mirai botnet and its variants and imitators are a wake-up call to the industry to better secure Internet of Things devices or risk exposing the Internet infrastructure to increasingly disruptive distributed denial-of-service attacks (Kolias, Kambourakis, Stavrou, & Voas, 2017). A simulation of what could happen if a botnet of Smart Meters was instructed to attack the central controlling server of an AMI is presented in (Sgouras, Birda, & Labridis, 2014).

Some Smart Meters are equipped with relays switches that can be remotely operated to disconnect the customer from the grid, consequently causing a local blackout (Anderson & Fuloria, 2010). While the identification of single malicious disconnect commands would be almost impossible, statistical analysis could be used to identify anomalous concentrations of such commands (Simonov, Bertone, Goga, & Terzo, Cyber Kill Chain Defender for Smart Meters, 2018).

4.3 Commercial solutions

There has been a trend towards the implementation of machine learning techniques for anomaly detection and prevention in the networks of the ICSs, not only on the academic field but also regarding the industry offering various commercial solutions.

DarkTrace’s Industrial Immune System for ICS implements a real-time defense for the OTs. The Industrial Immune System is a self-learning cyber AI technology that detects novel attacks and insider threats at an early stage. It is based on Bayesian probabilistic mathematics and leverages the capabilities of the of machine learning and AI algorithms. The technology operates like a human immune system which identifies subtle shifts in the expected behavior and has the ability to automatically fight against the intruders. It identifies the deviations from the learned pattern and alerts the organization to the potential threat. The self-learning technology is protocol agnostic and can be deployed across a range of OT environments, providing full coverage of the organization without disrupting daily operations. By monitoring from a central location, and deploying small probe appliances into substations, it protects entire power grids and utility systems. Regardless of network topology, a complete visibility of RTUs and remote OT across all substations and compressors is provided. The technology models and compares behavior of control system devices across all sites, detecting threats at the substation level, for both remote and local physical compromise.

ReaQta has developed an Endpoint Threat Response platform based on A.I. And machine learning algorithms which is able to detect new cyber threats, spanning from simple ransomware to more sophisticated in-memory only attacks. The solution automates and speeds up the detection and response process, minimizing the human interactions required. They have developed a NanoOS capable of acquiring data from the endpoints at the silicon level while completely isolating the security layer from attackers.

ElastiGRID of ECI provides a complete multiservice platform, supporting OT and IT services over the most appropriate transport and offers a holistic security suite that includes state of the art OT.

5. Conclusions

The gradual introduction of ICT and IoT technologies in the energy sector, and in particular the Smart Grid, introduces many positive effects that were not possible in the past. This nevertheless also introduces complexity and greatly increase the attack surface available to malicious actors. Most legacy systems, that are still used and will still be used for many more years, were not designed with security in mind and are particularly vulnerable to the opening of new attacks from the network connections. At the same time, in recent years we have witnessed the rise of dozens of threat groups, almost certainly for the most part following directives of some Nation-State, infiltrating the most various Critical Infrastructures creating continuous threats to the safety and security of society.

While security measures to mitigate the new threats are being introduced and partially reduce the risk of disruptive acts, too many breaches still occur and most of them remain undetected for months or years, and at times when it's already too late and the damages already happened.

Artificial Intelligence techniques can be helpful to enhance the detection rate and time of potential threats and ongoing attacks, avoiding or mitigating the impact of disruptive incidents.

It is however fundamental to always keep in mind that there is no such thing as a "silver bullet" and no security system is perfect. Artificial Intelligence technologies are no exception; they are just one step further in the direction of a better security. Carefully crafted data could even be used to trick and exploit AI algorithms to do harm. The past teaches us that highly motivated–and financed- actors can ideate the most sophisticated and creative ways to reach their objectives, overcoming no matter what advanced security mechanism.

References

FireEye. (2019). *M-Trends 2019.* FireEye.

Anderson, R., & Fuloria, S. (2010). Who Controls the off Switch? *2010 First IEEE International Conference on Smart Grid Communications.* Gaithersburg, MD: IEEE.

AV-TEST. (n.d.). *Malware Statistics & Trends Report.* Retrieved from AV-TEST: https://www.av-test.org/en/statistics/malware/

Bernabeu, E. E., & Katiraei, F. (2011). *Aurora Vulnerability: Issues & Solutions Hardware Mitigation Devices (HMDs).* Quanta Technology.

Blueliv. (2019). *Inside the Shamoon3 toolkit.* Blueliv.

BRONK, C., & TIKK–RINGAS, E. (2013). *Hack or Attack? Shamoon and the Evolution of Cyber Conflict.* THE JAMES A.BAKER IIIINSTITUTE FOR PUBLIC POLICY.

Bundock, R. (2015, November 2). *Organised crime and EU solidarity – Enel Italy talks cybersecurity.* Retrieved from Smart Energy International: https://www.smart-energy.com/interviews/enel-italy-talks-cybersecurity/

Collantes, M. H., & Padilla, A. L. (2015). *Protocols and network security in ICS infrastructures.* INCIBE.

Dragos. (2017). *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations.*Dragos.

Dragos. (2017). *TRISIS Malware: Analysis of Safety System Targeted Malware.* Dragos.

Durbhaka, G. K., & Selvaraj, B. (2016). Predictive maintenance for wind turbine diagnostics using vibration signal analysis based on collaborative recommendation approach. *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI).* Jaipur: IEEE.

ECSO. (2018). *ENERGY NETWORKS AND SMART GRIDS: Cyber security for the energy sector.* ECSO.

El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-Security in Smart Grid: Survey and Challenges. *Computers & Electrical Engineering*.

F-Secure. (2019). *The state of the station: A report on attackers in the energy industry.* F-Secure.

Gebraeel, N., Lawley, M., Liu, R., & Parmeshwaran, V. (2004). Residual life predictions from vibration-based degradation signals: a neural network approach. *IEEE Transactions onIndustrial Electronics*.

Gunduz, M., & Das, R. (2018). Analysis of cyber-attacks on smart grid applications. *2018 International Conference on Artificial Intelligence and Data Processing (IDAP).* Malatya: IEEE.

Hacquebord, F., & Pernet, C. (2019). *Drilling Deep: A Look at Cyberattacks on the Oil and Gas Industry.* Trend Micro.

INCIBE. (2017). *Security guide for Industrial Protocols - Smart Grid.* INCIBE.

Karimipour, H., Geris, S., Dehghantanha, A., & Leung, H. (2019). Intelligent Anomaly Detection for Large-scale Smart Grids. *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)* (pp. 1-4). Edmonton, AB, Canada: IEEE.

Kaspersky Lab. (2017). *From Shamoon to StoneDrill.* Kaspersky.

Kesler, B. (2011). The Vulnerability of Nuclear Facilities to Cyber Attack. *Strategic Insights*.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *Computer*.

Langner, R. (2013). *To Kill a Centrifuge.* Langner Group.

Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid.* E-ISAC.

Lopez, C., Sargolzaei, A., Santana, H., & Huerta, C. (2015). Smart Grid Cyber Security: An overview of Threats and Countermeasures. *Journal of Power and Energy Engineering*.

Marino, D. L., Wickramasinghe, C. S., Amarasinghe, K., Challa, H., Richardson, P., A. Jillepalli, A., Manic, M. (2019). Cyber and Physical Anomaly Detection in Smart-Grids. *2019 Resilience Week (RWS).* San Antonio, TX, USA: IEEE.

Mattioli, R., & Levy-Bencheton, C. (2014). *Methodologies for the identification of Critical Information Infrastructure assets and services.* ENISA.

Mohsenian-Rad, A.-H., & Leon-Garcia, A. (2011). Distributed Internet-Based Load Altering Attacks Against Smart Power Grids. *EEE Transactions on Smart Grid*.

Nelson, N. (2016). *The Impact of Dragonfly Malware on Industrial Control Systems.* SANS.

Otuoze, A., Mustafa, M., & Larik, R. (2018). Review Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology*.

Ponemon. (2019). *The Cost of Cybercrime.* Accenture.

Reed, T. C. (2004). *At the Abyss: An Insider's History of the Cold War.* Presidio Pr.

Rossi, B., Chren, S., Buhnova, B., & Pitner, T. (2016). Anomaly detection in Smart Grid data: An experience report. *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC).* Budapest: IEEE.

Sgouras, K. I., Birda, A. D., & Labridis, D. P. (2014). Cyber Attack Impact on Critical Smart Grid Infrastructures. *ISGT 2014.* Washington, DC: IEEE.

Shereen, E., & Dán, G. (2020). Model-Based and Data-Driven Detectors for Time Synchronization Attacks Against PMUs. *IEEE Journal on Selected Areas in Communications*.

Simonov, M., Bertone, F., & Goga, K. (2019). Detecting the Manipulation of Demand via IoT. *2019 5th International Conference on Event-Based Control, Communication, and Signal Processing (EBCCSP).* Vienna, Austria: IEEE.

Simonov, M., Bertone, F., Goga, K., & Terzo, O. (2018). Cyber Kill Chain Defender for Smart Meters. *Complex, Intelligent, and Software Intensive Systems. CISIS 2018.* Springer.

Simonov, M., Chicco, G., & Zanetto, G. (2017). Event-driven energy metering: Principles and applications. *IEEE Transactions on Industry Applications*.

Soltan, S., Mittal, P., & Poor, H. V. (2018). BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. *USENIX Security Symposium 2018*.

Tofan, D., NIKOLAKOPOULOS, T., & Darra, E. (2016). *The cost of incidents affecting CIIs.* ENISA.

Vanraj, Goyal, D., Saini, A., Dhami, S. S., & Pabla, B. S. (2016). Intelligent predictive maintenance of dynamic systems using condition monitoring and signal processing techniques — A review. *2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA).* Dehradun: IEEE.

Wallace, B., & McClure, S. (2014). *Operation Cleaver.* Cylance.