# Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures

Leandros Maglaras[1,2,*], Mohamed Amine Ferrag[3,4], Abdelouahid Derhab[5], Mithun Mukherjee[6], Helge Janicke[1], Stylianos Rallis[2]

[1]Cyber Security Center, De Montfort University, Leicester, LE1 9BH, UK
[2]General Secretariat of Digital Policy, Ministry of Digital Policy Telecommunications and Media, Athens, Greece
[3]LabSTIC Laboratory, Guelma University, 24000 Guelma, Algeria
[4]LRS Laboratory, Badji Mokhtar-Annaba University, 23000 Annaba, Algeria
[5]Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia
[6]Guangdong University of Petrochemical Technology, Maoming 525000, China

## Abstract

As Critical National Infrastructures are becoming more vulnerable to cyber attacks, their protection becomes a significant issue for any organization as well as a nation. Moreover, the ability to attribute is a vital element of avoiding impunity in cyberspace. In this article, we present main threats to critical infrastructures along with protective measures that one nation can take, and which are classified according to legal, technical, organizational, capacity building, and cooperation aspects. Finally we provide an overview of current methods and practices regarding cyber attribution and cyber peace keeping.

## 1. Introduction

Cyber security is currently one of the main concerns for Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) operators. In fact, SCADA systems collect the data and monitor the automation processes, which are visualized to the operators of the system via human-to-machine interfaces. The operators can take control of the system remotely and issue commands such as opening a valve, setting a temperature point or starting/stopping a pump [1]. Recently, several countries have witnessed the impact of cyber threats to the critical infrastructures [2]. For example, in December 2015, Ukraine was hit by massive power outage due to an outcome of SCADA cyber attack [3]. This caused about 230K people out of power for several hours. Another attack that was reported in 2016, although happened in 2013, targeted a small dam in Rye Brook, New York [4]. Based on a joint report by FBI and homeland security, the Wolf Creek Nuclear Operating Cooperation was targeted [5] in 2017. Although the nature of the attack was unknown, the impact could go beyond any nation. Recently, UK's general communications head quarters (GCHQ) and National Cyber Security Centers (NCSC) are concerned about suspicious attacks on UK energy sectors [6]. The above are some of the examples, however, these cyber attacks can be related to any critical infrastructure, such as oil and gas industry, traffic signal, water sewage building, transportation, and digital infrastructure.

It is often observed that critical national infrastructures (CNI) are controlled, even in part, by private-sector companies. Therefore, cyber defence of any nation has to play a significant role in privately operated networks for the CNI. Many SCADA applications are nowadays using common operating systems such as Windows as well as well-known and vulnerable protocols like Transport Control Protocol (TCP). The security vulnerabilities are

---

*Corresponding author. Email: leandros.maglaras@dmu.ac.uk

publicly available and famous events like Black Hat are now discussing more about industrial systems, proving that hackers are also focusing on these systems [7]. Moreover, CNIs continue to suffer information security incidents and breaches as a result of human errors even though humans are recognised as the weakest link with regard to information security [8].

*Lifecycle of Cybersecurity:* Similar to other information technology (IT) processes, cyber security often follows a lifecycle model of prediction, protection, detection, and reaction. The details are discussed as follows:

1. During the *prediction phase,* each organization (or nation) needs to consider all proactive measures to identify potential attackers along with their intentions and the methods that they are going to use. This step can be implemented by collecting cyber threat intelligence and conducting risk management [9]. Defining scope and objectives for Risk Management, the external and internal environment of CNIs, conducting a risk assessment and producing appropriate risk mitigation plans are all steps that need to be taken, following a standardized methodology, e.g. ISO 31000.

2. During protection phase, the organization applies hardware and software measures that are needed in order to accomplish its security goals, following the results of the risk assessment phase.

3. During the detection phase, the organization needs to implement monitoring mechanisms along with intrusion detections systems [10], which can distinguish legitimate from abnormal behavior or normal from malicious network traffic inside the system.

4. The last phase of cyber security lifecycle includes all the processes and methods that the organization (or nation) needs to have in place for incident notification and management, along with appropriate mitigation, recovery, and business continuity plans. In the core of the cyber security lifecycle lies the cyber threat intelligence, which is the process of collecting data and deriving meaningful information for the system.

SCADA systems are nowadays the targets of cyber attackers, and it is worthwhile to note that attacking them affects a substantial number of persons, potentially causing significant damage and ultimately threatening human lives [11]. Post-event investigation has frequently linked these attacks to the exploitation of vulnerabilities deeply rooted in the ICS design philosophy which focuses on availability rather than security.

In this article, we summarize the main issues in regulations for cyber security and outline several aspects of policy making to tackle cyber attacks on the CNIs. The rest of the paper is organized as follows. Section 2 discusses the main threats that critical infrastructures (CI) are facing today. Section 3 presents several measures for the protection of CI. Techniques for cyber attack attribution are discussed in Section 4. Finally, conclusions are drawn in Section 5.

## 2. Threats to Critical Infrastructures

Vulnerability assessment of cybersecurity is identified by five main phases, namely, 1) Identify the threat model, 2) Identify possible vulnerabilities of the attack, 3) Identify intrusion scenarios , 4) Compute scenario vulnerability, and 5) Decision-making, as presented in Fig. 1.
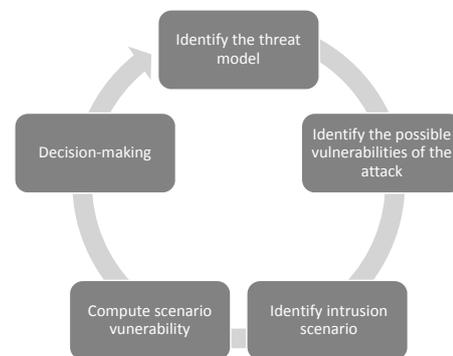


**Figure 1.** Procedures of vulnerability assessment of cybersecurity for critical infrastructures

In order to evaluate vulnerability indices on cybersecurity of critical infrastructures, Ten et al. [12] proposed two main procedures, namely, 1) cybersecurity conditions and 2) evaluation of vulnerability indices. The cybersecurity condition assessment is measured by a number $X$, which assumes the value of 0.33, 0.67, or 1. A low value indicates that the system condition is invulnerable, while the value 1 indicates that the system is vulnerable. For the second procedure, the authors proposed four steps to assess the security vulnerability, namely, 1) identifying the intrusion scenarios; 2) evaluating vulnerability indices for the system, intrusion scenarios, and attack leaves; 3) port auditing; and 4) password strength evaluation.

Since we are moving to the era of IoT, there are two categories of attacks:

- The attacks on back-end IoT devices. This category of attacks is connected directly with critical infrastructures. Under this category, we can find the following attacks: attacks on SCADA systems and attacks analysis for critical infrastructure.
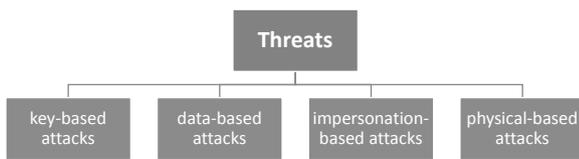
**Figure 2.** Classification of threats for SCADA system in Smart Grids

- The attacks based on end-user IoT devices. This category of attacks is not connected directly with critical infrastructures. Under this category, we can find the following attacks: IoT-enabled attack vectors, IoT-enabled attacks on healthcare critical infrastructure, IoT-enabled attacks on intelligent transportation systems, IoT-enabled attacks on 5G cellular infrastructure.

## 2.1. Attacks on SCADA systems

SCADA systems and substations are now interconnected with other systems thanks to the Power System Communication (PSC) systems [13]. SCADA system is the core of smart grid decision making. This interconnection between SCADA system and smart grid creates new possibilities and threats. Classification of threats in smart grids is done using different criteria such as passive or active, internal or external, etc.

In [14], authors classified threats in smart grids into four categories, including, (1) key-based attacks, (2) data-based attacks, (3) impersonation-based attacks, and (4) physical-based attacks, as presented in Fig. 2. In order to detect attacks against critical infrastructures, Zonouz et al. [15] proposed a cyber-physical security state estimation framework, named SCPSE, which estimates the cyber-physical security state of a power grid. The SCPSE framework uses stochastic information fusion algorithms and merges sensor information from both cyber and electrical infrastructures. By using information provided by alerts from intrusion detection systems, the SCPSE framework can identify malicious measurement corruptions.

## 2.2. Attack analysis for critical infrastructure

Several techniques use the attack tree model to analyze the attacks targeting the critical infrastructures, as discussed by Fujita et al. [16]. Specifically, the authors proposed a systemic integration of granular computing and resilience analysis for critical infrastructures. This resilience analysis uses three tools, namely, 1) Three-way decisions as a tool for cognitive analysis, 2) Granular structures based on binary relations, 3) An approach based on the hierarchical granular modeling; and 4)

Dominance-based rough sets as a tool to understand what are the parts of a critical infrastructure that are not performing well.

## 2.3. IoT-enabled attack vectors

Modeling of IoT-enabled attack vectors against critical infrastructures and services, as proposed by Stellios et al. [17], contains three main entities, namely, 1) adversary, 2) IoT device, and 3) actual target.

- The adversary is characterized by the following three capabilities: required access to the IoT, technical skills, and required motivation.

- IoT vulnerabilities are categorized by embedded vulnerabilities and network vulnerabilities.

- The connectivity between the IoT device and the actual target is categorized by the following two types: Direct connectivity with a critical system, and indirect connectivity with a critical system.

## 2.4. IoT-enabled attacks on healthcare critical infrastructure

According to Gope and Hwang [18], IoT-enabled attacks on healthcare critical infrastructure can be classified into three types of attack assumptions, namely, 1) Computational capabilities, 2) Listening capabilities, and 3) Broadcasting capabilities.

- With computational capabilities, an adversary can launch data modification and impersonation attacks.

- By using listening capabilities, an attacker can perform eavesdropping and tracking of healthcare critical infrastructure.

- Based on broadcasting capabilities, an attacker can replay critical data of a healthcare critical infrastructure.

## 2.5. IoT-enabled attacks on intelligent transportation systems

For modeling IoT-enabled attacks on intelligent transportation systems, Petit and Shladover [19]categorized attackers in an automated vehicle system as, 1) Internal versus external, 2) Malicious versus rational, 3) Active versus passive, 4) Local versus extended, and 5) Intentional versus unintentional. For future autonomous automated vehicles, the following attack surfaces can be considered:

- Infrastructure sign

- Machine vision

- Global positioning system

- In-vehicle devices

- Acoustic sensors

- Radar

- Light detection and ranging

- Material/structure on which the vehicles drive

- In-vehicle sensors

- Odometric sensors

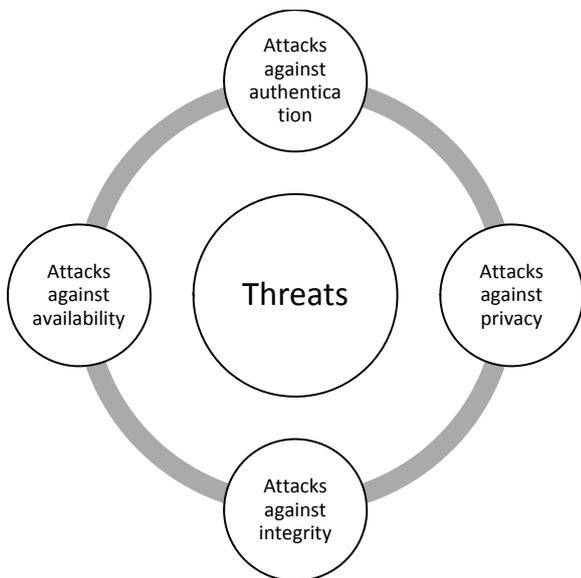- Electronic devices

- Maps for longitudinal and lateral directions



**Figure 3.** Classification of threats for 5G cellular infrastructure

## 2.6. IoT-enabled attacks on 5G cellular infrastructure

In general, a central base station cannot determine the behavior of the users in 5G cellular infrastructure. According to Geraci et al. [20], the confidential messages in 5G cellular infrastructure can be eavesdropped by both: (i) users in the same cell and (ii) users in other cells.

In [21], authors classified IoT-enabled attacks on 5G cellular infrastructure into four categories, including, (1) attacks against privacy, (2) attacks against integrity,

(3) attacks against availability, and (4) attacks against authentication, as presented in Fig 4. Ahmad et al. [22, 23] in another interesting article provided an overview of different types of IoT-enabled attacks on 5G cellular infrastructure according to target point/network element, which can be SDN controller-switch communication, subscriber location, virtual resources, hypervisor, shared cloud resources, open air interfaces, unencrypted channels...etc.

## 3. Protection of Critical Information Assets

In this section, we propose some measures for the protection of Critical Infrastructure. The measures are divided into two main categories: *cyber security measures* and *cyber threat intelligence*.
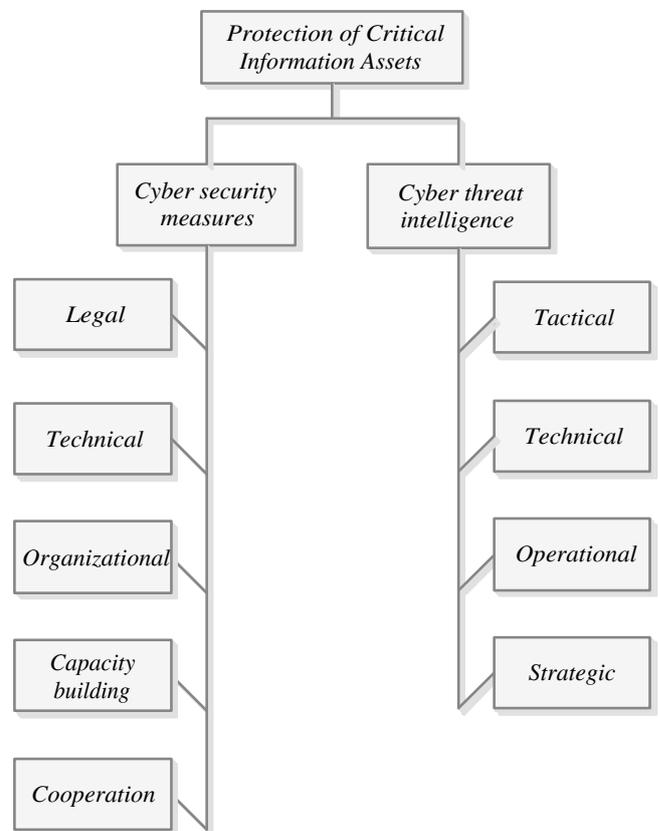


**Figure 4.** Measures for the protection of critical information assets

## 3.1. Cyber security measures

They are classified with respect to: legal, technical, organizational, capacity building, and cooperation aspects, as defined by the International Telecommunication Union (ITU) [24, 25].

- **Legal measures** aim to provide legislations and an implementable regulatory framework to protect the cyber space. As for CI, the following good practices can be recommended:

    – Ensure mandatory periodic assessment of CIs through information security audits

    – Check the compliance of software and hardware tools, which are used in the CI, with recognized security standards such as: ISO 27001.

- **Technical measures** consider the technological tools (software and hardware) to prevent, detect, mitigate, and respond to cyber attacks, such as:

    – Implementation of internationally recognized security standards within organizations, especially the critical infrastructure ones.

    – Implementation of preventive and detective security tools such as: firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Antivirus/ Anti-malware.

    – Implementation of measures for physical security, access control, patching and upgrading, and forensics.

    – Development of an incident response capability.

- **Organizational measures** are important for the proper implementation of any type of national initiative or policy. Under this aspect, we recommend the following:

    – Develop a national critical infrastructure protection policy.

    – Develop a national framework for the implementation, evaluation, and maintenance of the cyber security policies.

    – Define an information security program for organizations.

    – Develop a national contingency plan.

    – Identify a national agency for the implementation of the critical infrastructure protection policy.

    – Conduct a national exercise to assess the cyber resilience of the CI.

    – Conduct security audits by organizations to check their cyber security preparedness.

- **Capacity building measures** aim to enhance knowledge and know-how in order to promote cyber security. Under this aspect, we recommend the following:

    – Encourage IT specialists in CI sectors to be certified under internationally recognized cyber security programs.

    – Conduct periodic awareness and training programs for employees.

- **Cooperation measures** aim to establish partnership between different stakeholders to increase cyber resilience of the organizations against cyber threats. Under this aspect, we recommend the following:

    – Establish trusted information sharing mechanisms on threats and vulnerabilities between private and public stakeholders

    – Establish a cooperation framework between industry and research to promote cyber security and increase resiliency against cyber attacks.

    – Build a cooperation framework between countries on different aspects related to cyber security.

    – Contribute in international efforts to protect the cyber space

## 3.2. Cyber threat intelligence

Cyber threat intelligence refers to the collection of inteligence before a cyber attacker targets a victim system. The purpose is to help organizations understand and mitigate the risks related to zero-day exploits, Advanced Persistent Threats (APTs), internal and external threat actors. This allows organizations to adopt a proactive cybersecurity approach, and take preventive countermeasures in advance. Inteligence can be gathered from different sources such as: open source intelligence (OSINT), social media intelligence (SOCMINT), human Intelligence (HUMINT), technical intelligence, and intelligence from the deep and dark web. The United Kingdom's National Cyber Security Centre (NCSC) classifies threat intelligence into the following four classes [26]:

- **Tactical Cyber threat intelligence**: This data is obtained from real-time monitoring of systems. It refers to real-time events and information related to adversary's actions inside the organization. Tactical threat intelligence is consumed by defenders to ensure that their incident response

systems and investigations are prepared for the tactics.

- **Technical Cyber threat intelligence**: This data is consumed through technical means, e.g., suspected malicious IP address. It has a short lifetime as an adversary can for example change the IP address. Technical threat intelligence generally helps the the defenders to take preventive actions, e.g., blocking the suspected IP address.

- **Operational Cyber threat intelligence**: This data gives details about a specific incoming attack such as: campaigns, malware, or cyber-weapon tools. It gives insignts that can guide and support the response to specific incidents, and help assessing the ability of the organization in determining future cyber threats·

- **Strategic Cyber threat intelligence**: This data represents high-level information and a timely warning of cyber threats, which is consumed at the board level or by other senior decision-makers. Strategic cyber threat intelligence forms an overall picture of the intention and capabilities of malicious cyber actors and their impact on high-level business decisions.

## 4. Attribution of Cyber Attacks

When a cyber attack is launched against a CI, it is likely that some real-world physical revelation will follow [1]. In some instances this could even lead to physical damage, injury, environmental effects or even loss of life. According to international or national law [27], legal or regulatory investigation may be required, increasing the importance of attribution artefacts. According to NIS directive, each Member State shall designate one or more national competent authorities for the security of network and information systems that can take the leading role in securing CIs. The responsible authority of the country will have to identify whether the incident was caused by an error in the operations, maybe a fault component, or whether the processes or devices were maliciously manipulated. Artefacts should be collected and kept in a way that both authenticity, integrity and usability are guaranteed.

Researchers have surveyed individual technical approaches to attribution, including; traceback - where the traffic from a target device is recursively steppedback through its routing path to its originating source, honey-pots - where vulnerable software and services are hosted in order to allow activities to be monitored among others.

**Traceback** is a class of methods that encompasses techniques by which the traffic from a target device is recursively stepped-back through its routing path to its originating source device [28]. Traceback can be supported by manual methods of traffic tracing or logging techniques supported from network devices. There is a third category of traceback that includes various methods of Probabilistic Packet Marking (PPM) [29], and ICMP traceback (iTrace) [30].

**Honeypots** approach the issue of attribution of attacks differently to Traceback methods. A honeypot is a system, or set of systems, where vulnerable software and services are hosted in order to allow activities to be monitored and logged. Several researchers have proposed the use of honeypots to protect important assets of critical infrastructure [31]. However, most of these honeypots are static systems that wait for the attackers. In order to increase the efficiency of honeypots they need to be as realistic as possible. In [32] authors introduce a honeypot network traffic generator that mimics a genuine control system in operation.

**Digital Forensics** is a broad subject which involves the recovery, acquisition and investigation of digital evidence. One technique that could be used is live forensics where data acquisition takes place while the system is operational. In order to avoid system crash, especially for the SCADA systems that exist in the core of each CI, authors in [33] propose the use of fail over systems. In either case post incident investigator will compete with recovery efforts, which will most likely destroy evidence.

**Network Forensics** field primarily involves two stages: collecting network messages and analyzing network messages. An organization must identify points in the network where they wish to collect network data. Again special care should be given regarding SCADA operation requirements [34].

**Malware Analysis** can be split into two areas: behavioural analysis and code analysis. Behavioral analysis examines the way that malware interacts with the environment [35] while code analysis examines the code that makes up the malware [36].

Measuring the performance of attribution attacks is an open issue although several methods have been proposed [37]. The development of modelling strategies for evaluating cyber attacks [38] are also important. Cook et al. [39] have used six individual metrics, as summarized in Table 1, to measure the effectiveness of each attribution in the context of ICS that can be applied to CIs.

Attacks may sometimes originate from another nation and attribution becomes a question of which country or law enforcement agency has the responsibility and authority to investigate, under which legal framework the perpetrators can be prosecuted, and which laws apply.

| Metric | Description |
|---|---|
| Performance | Ability to provide attribution functions without degrading CI performance |
| Reliability | Ability to provide attribution without affecting operating and safety processes |
| Extent | Ability to monitor traffic to provide a full picture of network behaviour |
| Coherence | Cross-reference traffic with device behaviours to permit inspection of command execution |
| Identification | Ability to identify the attacker from behaviours or technical signatures |
| Intent | Ability to determine the purpose of the attack in order to support a prosecution |

**Table 1.** Metrics of attribution

This transnational issue was analyzed in the Tallinn Manual on the International Law Applicable to Cyber Warfare [40]. In the same context authors in [41] argued that as cyber warfare becomes an increasing part of wider conflict, peacekeeping organizations such as the United Nations will probably need to perform cyber peacekeeping.

In order to perform cyber peacekeeping, UN or the competent international body, should also consider peace enforcement in order to protect civilians. While such an event seems valuable, the feasibility is be questionable. Research into cyber warfare [42] has shown that there is still no answer to questions such as what constitutes an armed attack in the cyber space or what the ethical boundaries of cyber warfare are. In the cyber domain, it is difficult to foresee the Security Council of th UN agreeing to enforce peace based upon a cyber conflict [43]. In depth study of how cyber peace enforcement could work and the value it could bring would be useful.

A big challenge is the technical challenges CNI presents. Facilities such as power plants and water facilities have properties, which make observation and monitoring more challenging than standard network monitoring techniques [37]. The use of proprietary protocols, air-gapping and a 24/7 availability requirement means that monitoring of events on these systems will require a specialised set of skills that are in high demand globally. A discussion on how the right expertise can be secured in the necessary numbers, and at a price that is within an operation's budget is a necessary future research topic.

Multi-lateral cooperation can be used in order to detect attacks and perform attribution, because even the largest intelligence organizations have limited human, technological and budgetary capacities to achieve global coverage [44]. US has established already after World War II the declassified 5-eyes cooperation with UK, Canada, Australia and New Zealand and in response to 9/11 a wider cooperation the 9-eyes cooperation including Denmark, France, Netherlands and Norway and finally the 14-eyes cooperation additionally including Belgium, Italy, Spain, Sweden and Germany.

## 5. Conclusions

As CNIs are vulnerable to cyber attacks, their protection becomes a significant issue for any nation as well as an organization. In this article, we have summarized the primary attributes of cyber attacks to the critical infrastructures. We have further provided the protective cyber security measures that one nation can take, and which are classified according to legal, technical, organizational, capacity building, and cooperation aspects. Cyber threat intelligence is also an important protection aspect as it helps taking countermeasures in advance, and enables developing a proactive and predictive cyber security posture. Attribution of cyber attacks, especially when the latter originate from another nation, is questionable regarding which country or law enforcement agency has the authority to investigate and prosecute the penetrators and cyber peacekeeping is foreseen to become a reality.

## References

[1] Leandros A Maglaras, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, and Tiago J Cruz. Cyber security of critical infrastructures. *ICT Express*, 2018.

[2] Cyber attack led to bristol airport blank screens. https://www.bbc.com/news/uk-england-bristol-45539841, Accessed: 2018-09-26.

[3] Ukraine cyber attack energy. https://www.wired.com/story/crash-override-malware/. Accessed on 05-Feb-2018.

[4] Rye dam attack. https://www.newsweek.com/cyber-attack-rye-dam-iran-441940. Accessed on 05-Feb-2018.

[5] Wolf creek nuclear plant hit cyberattack. https://www.theenergytimes.com/cybersecurity/wolf-creek-nuclear-plant-hit-cyberattack. Accessed on 05-Feb-2018.

[6] Energy sector on alert for cyber attacks on uk power network. https://www.ft.com/content/d2b2aaec-4252-11e8-93cf-67ac3a6482fd. Accessed on 05-Feb-2018.

[7] Eric D Knapp and Joel Thomas Langill. *Industrial Network Security: Securing critical infrastructure networks*

for smart grid, SCADA, and other Industrial Control Systems. Syngress, 2014.

[8] Mark Evans, Ying He, Leandros Maglaras, and Helge Janicke. Heart-is: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, 2018.

[9] Patricia AS Ralston, James H Graham, and Jefferey L Hieb. Cyber security risk assessment for scada and dcs networks. *ISA transactions*, 46(4):583–594, 2007.

[10] Leandros A Maglaras and Jianmin Jiang. Intrusion detection in scada systems using machine learning techniques. In *Science and Information Conference (SAI), 2014*, pages 626–631. IEEE, 2014.

[11] Allan Cook, Richard Smith, Leandros Maglaras, and Helge Janicke. Measuring the risk of cyber attack in industrial control systems. BCS eWiC, 2016.

[12] Chee-Wooi Ten, Govindarasu Manimaran, and Chen-Ching Liu. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEEE Trans. Syst. Man, Cybern. - Part A Syst. Humans*, 40(4):853–865, jul 2010.

[13] Göran N Ericsson. Cyber security and power system communication—essential parts of a smart grid infrastructure. *IEEE Trans. on Power Delivery*, 25(3):1501–1507, 2010.

[14] Mohamed Amine Ferrag, Leandros A Maglaras, Helge Janicke, Jianmin Jiang, and Lei Shu. A systematic review of data protection and privacy preservation schemes for smart grid communications. *Sustainable Cities and Society*, 38:806–835, 2018.

[15] Saman A Zonouz, Katherine M Rogers, Robin Berthier, Rakeshbabu Bobba, William H Sanders, and Thomas J Overbye. Scpse: Security-oriented cyber-physical state estimation for power grid critical infrastructures. *IEEE Trans. Smart Grid*, 3(4):1790–1799, 2012.

[16] Hamido Fujita, Angelo Gaeta, Vincenzo Loia, and Francesco Orciuoli. Resilience analysis of critical infrastructures: a cognitive approach based on granular computing. *IEEE Trans. on Cybernetics*, pages 1–14, 2018.

[17] Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcaraz, and Javier Lopez. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, 2018.

[18] Prosanta Gope and Tzonelih Hwang. Bsn-care: A secure iot-based modern healthcare system using body sensor network. *IEEE Sensors Journal*, 16(5):1368–1376, 2016.

[19] Jonathan Petit and Steven E Shladover. Potential cyberattacks on automated vehicles. *IEEE Trans. Intelligent Transportation Systems*, 16(2):546–556, 2015.

[20] Giovanni Geraci, Harpreet S Dhillon, Jeffrey G Andrews, Jinhong Yuan, and Iain B Collings. Physical layer security in downlink multi-antenna cellular networks. *IEEE Transactions on Communications*, 62(6):2006–2021, 2014.

[21] Mohamed Amine Ferrag, Leandros Maglaras, Antonios Argyriou, Dimitrios Kosmanos, and Helge Janicke. Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, 101:55 – 82, 2018.

[22] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. Overview of 5g security challenges and solutions. *IEEE Communications Standards Magazine*, 2(1):36–43, 2018.

[23] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. 5g security: Analysis of threats and solutions. In *Standards for Communications and Networking (CSCN), 2017 IEEE Conference on*, pages 193–199. IEEE, 2017.

[24] S Brahima. Global cybersecurity index 2017. *International Telecommunication Union (ITU)*, pages 1–77, 2017.

[25] Ismael Peña-López et al. Global cybersecurity index & cyberwellness profiles. 2015.

[26] D Chismon and M Ruks. Threat intelligence: Collecting, analysing, evaluating. *MWR InfoSecurity Ltd*, 2015.

[27] Leandros Maglaras, George Drivas, Kleanthis Noou, and Stylianos Rallis. Nis directive: The case of greece. *EAI Endorsed Transactions on Security and Safety*, 18:5, 2018.

[28] Vadim Kuznetsov, Helena Sandström, and Andrei Simkin. An evaluation of different ip traceback approaches. In *International Conference on Information and Communications Security*, pages 37–48. Springer, 2002.

[29] Dawn Xiaodong Song and Adrian Perrig. Advanced and authenticated marking schemes for ip traceback. In *Proc. IEEE INFOCOM Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 2, pages 878–886, 2001.

[30] Steven Michael Bellovin, Marcus Leech, and Tom Taylor. Icmp traceback messages. 2003.

[31] Paulo Simões, Tiago Cruz, Jorge Gomes, and Edmundo Monteiro. On the use of honeypots for detecting cyber attacks on industrial control networks. In *Proc. 12th Eur. Conf. Inform. Warfare Secur. ECIW 2013*, 2013.

[32] Htein Lin, Stephen Dunlap, Mason Rice, and Barry Mullins. Generating honeypot traffic for industrial control systems. In *International Conference on Critical Infrastructure Protection*, pages 193–223. Springer, 2017.

[33] Irfan Ahmed, Sebastian Obermeier, Martin Naedele, and Golden Richard III. Scada systems: challenges for forensic investigators. *Computer*, page 1, 2012.

[34] Abdun Naser Mahmood, Christopher Leckie, Jiankun Hu, Zahir Tari, and Mohammed Atiquzzaman. Network traffic analysis and scada security. In *Handbook of Information and Communication Security*, pages 383–405. Springer, 2010.

[35] Jayant Shukla. Application sandbox to detect, remove, and prevent malware, January 17 2008. US Patent App. 11/769,297.

[36] Ulrich Bayer, Andreas Moser, Christopher Kruegel, and Engin Kirda. Dynamic analysis of malicious code. *Journal in Computer Virology*, 2(1):67–77, 2006.

[37] Andrew Nicholson, Tim Watson, Peter Norris, Alistair Duffy, and Roy Isbell. A taxonomy of technical attribution techniques for cyber attacks. In *European Conference on Information Warfare and Security*, page 188, 2012.

[38] Kosmas Pipyros, Christos Thraskias, Lilian Mitrou, Dimitris Gritzalis, and Theodoros Apostolopoulos. A new strategy for improving cyber-attacks evaluation in the context of tallinn manual. *Computers & Security*, 74:371–383, 2018.

[39] Allan Cook, Andrew Nicholson, Helge Janicke, Leandros Maglaras, and Richard Smith. Attribution of cyber attacks on industrial control systems. 2016.

[40] Michael N Schmitt. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.

[41] Michael Robinson, Kevin Jones, Helge Janicke, and Leandros Maglaras. An introduction to cyber peacekeeping. *Journal of Network and Computer Applications*, 114:70–87, 2018.

[42] Michael Robinson, Kevin Jones, and Helge Janicke. Cyber warfare: Issues and challenges. *Computers & security*, 49:70–94, 2015.

[43] Michael Robinson, Kevin Jones, Helge Janicke, and Leandros Maglaras. Developing cyber peacekeeping: Observation, monitoring and reporting. *arXiv preprint arXiv:1806.02608*, 2018.

[44] Klaus Saalbach. Attribution von cyber-attacken - methoden und praxis. 2017.