Advances in Manufacturing Technology XXXV
M. Shafik and K. Case (Eds.)
© 2022 The authors and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License 4.0 (CC BY-NC 4.0).
doi:10.3233/ATDE220599

Identifying and Predicting Cybersecurity Threats in Industry 4.0 Based on the Motivations Towards a Critical Infrastructure

Adel ALQUDHAIBI, Abdulmohsan ALOSEEL, Sandeep JAGTAP and Konstantinos SALONITIS
School of Aerospace Transport and Manufacturing, Cranfield University, MK43 0AL, UK.

Abstract. Industry 4.0 (I4.0) is an emerging concept describing the business setting application of a broad set of digitalisation technologies, connectivity, and automation. The most common critical infrastructure (CI) uses Industrial Control Systems (ICS) for operation and supervisory control. However, the Supervisory Control and Data Acquisition (SCADA) and Internet of things (IoT) systems are examples of ICSs applications. These systems, like any other systems exposed to many security risks and are vulnerable to many threats. This is mainly due to the lack of objective standards and proactive security countermeasures that companies unintentionally neglected in the early stages of designing these systems. It is also due to the absence of managerial and technical skills necessary to implement them. Therefore, identifying and preventing potential security threats against CIs is the focus of this paper. A novel security approach concept that can predict cybersecurity threats based on the CI nature and take into consideration the attack motivations accordingly has been delivered in this paper. The proposed concept of this approach will also facilitate the detection of potential attack types and the required countermeasures in particular infrastructures.

Keywords: Cybersecurity, Critical Infrastructure (CI), Digitalisation, Motivations, Industry 4.0, Manufacturing.

1. Introduction

Industry 4.0 (I4.0) is a new term that refers to the use of a wide range of digitalised technologies, connectivity, and automation in a business setting. These technologies include the Internet of Things (IoT), the Industrial Internet of Things (IIoT), cloud computing, big data, artificial intelligence, machine learning, new generation robotics and blockchain. New business models using smart products are emerging, calling for a shift towards digital services and manufacturing. Thanks to customer–supplier data sharing and advanced analytics, supply chains are becoming more flexible and agile in this environment. However, despite the advantages of digitalising industry sector services, this digitalisation opens the door to numerous security risks and vulnerabilities.

Therefore, in the context of I4.0, cybersecurity plays a vital role in preventing companies from losing their competitiveness [1], as Critical infrastructure (CI) is

vulnerable to cyber-attacks that can affect entire business models. According to the Cisco 2018 annual cybersecurity report [2], 31% of organisations have experienced cyber-attacks on operational technology, while 38% expect attacks to extend from information technology to operational technology. Although 75% of experts perceive cybersecurity as a priority, only 16% say their companies are well prepared to face cybersecurity challenges [3]. It is due to the lack of objective standards that companies can refer to and the lack of managerial and technical skills necessary to implement them.

CI is one of the essential pillars of developed countries globally and provides energy, electricity, water, health, education, transportation and defence services. Therefore, ensuring the stability of CI functionality is vital, and any malfunction may result in catastrophic consequences. The Commission of the European Union categorises CI into several categories: energy, information communication technology, water, food, health, financial, public & legal order and safety, civil administration, transport, chemical and nuclear industry, space and research [4]. Predicting cyber-attacks in advance and prioritising security countermeasures and controls for the most critical vulnerabilities are crucial tools in securing these systems against potential cyber-attack.

In the context of cyber-attack and machine learning, the prediction concept refers to the output of a prediction model that is based on three main elements: (1) the algorithm, (2) the datasets and (3) the features of the data. The prediction model processes the designated algorithm, enters data and data features and forecasts a particular outcome in terms of potential attack existence [5]. The following sections define the data required for the proposed approach. In this paper, only the initial concept is defined and proposed; the implementation will be outlined in future work along with a developed Python code.

2. A proposed security approach for predicting cyber-attacks in critical infrastructures (the PCCI approach)

This section outlines the concept of predicting cyber-attacks in critical infrastructure (PCCI). By recognising different sectors of infrastructure, it can be determined that attackers' motivations vary according to the target. The adopted method used in developing the PCCI approach and the main components of the PCCI was based on the extraction and synthesis of the influencing factors stated in literary reviews. In terms of implementation, several machine learning algorithms, such as decision tree classifiers and support vector machines, will be examined in future work. Having determined the influencing factors affecting CI cybersecurity, the basic principles on which this approach is based can be defined. They are as follows:

2.1. The purpose of the critical infrastructure

In the past few decades, there has been a tremendous proliferation of CI, including IoT, IIoT, supervisory control and data acquisition (SCADA) systems and many other cyber-physical systems. The linking of these systems' functions to the internet reflects one of the most important aspects of I4.0. This remarkable development opened the door to countless applications that have contributed significantly to increased citizen welfare by allowing higher quality services in the health, education, banking and public transport sectors. Additionally, in the industrial, armaments and military sectors, I4.0 has significantly impacted applications and solutions, and, as a result, production efficiency has drastically increased. Furthermore, due to I4.0's connection to the internet, its

automation and remote monitoring have made it possible to control and operate these systems remotely and without human intervention. However, this tremendous development has created cybersecurity risks and digital threats that could have catastrophic consequences. Taking CI design as well as specific infrastructure services into account enables the prediction of potential cyber-attacks. CI functionality must be dependable in the United States. Therefore, the vulnerability of CI systems, the economy, the nation's security, and public safety and health has increased due to cybersecurity threats.

2.2. Attacker's & adversary motivations.

Having considered the CI design and the services it provides, it is possible to predict an attacker's method, as methods differ from sector to sector. For example, methods of attack on the military are espionage, eavesdropping and surveillance.

Several studies [6,7] have addressed the motivations behind cyberattacks, which might be military, financial or for the purpose of commercial profit or privacy breaches. Not all adversary motivations are similar, and, in some cases, there may be more than one motivation behind a cyberattack [8]. For instance, the cyberwar between Russian and Ukrainian hackers carries inside it many motivations [9]. A part of the PCCI approach is to predict these scenarios in advance. The ability to implement this approach depends on the business needs of CI. Table 1 summarises different motivations based on CI type [7], [10], [11].

Table 1: CI and adversary motivations.

No.	Critical Infrastructures	Motivations
1.	Financial (Retailers, Banking) and Health.	Financial profit
2.	Civil administration, Energy, Food, Water, Chemical, and nuclear industry.	War/Defence
3.	Information, Communication Technology	Social/Political
4.	Public & Legal Order and Safety, Transport	Nuisance/Destruction
5.	Space and Research, Civil administration	Espionage
6.	Energy, Food, Water, and Information.	Revenge

Attackers undoubtedly have a diverse range of experiences and skills. Additionally, they appear to be driven by various motivations and causes. These motivations and the anonymous nature of the internet, which frequently hides these motivations until it is too late, make the problem of network security more challenging [12]. In many cases, there has been no reliable evidence to prove who was behind cybercrimes or cybersecurity incidents. The provision of evidence-based knowledge of potential threats is called threat intelligence. Merging adversary motivations with threat intelligence improves the efficiency and effectiveness of predicting and preventing cybersecurity threats. Linking specific infrastructure services to attackers' motivations enables the prediction of potential attack types and their tools, methods, and techniques.

2.3. Security threats predication & Potential attack methods

Taking infrastructure design into account facilitates the prediction of attacker motivations and methods against the cybersecurity goals of confidentiality, integrity and availability.

There are many security risks, and studies have discussed these in detail. The security risks differ between threats, attacks, vulnerabilities and exposure. Each type of security risk has its specific tools, methods, and techniques of execution. Therefore, predicting the plan of attack based on the motivations related to specific CI services significantly facilitates the identification of security risks, and thus, the necessary security countermeasures can be taken efficiently and effectively. The following table summarises some of the attack methods against different CI [7], [11].

Table 2. Describing several CIs, the motivations, and the attack methods.

No.	Critical Infrastructures	Motivations	Attack Methods
1.	Energy, Water, Food, Transport.	Social/Political.	Distributed Denial of Service (DDoS), Brute force attack.
2.	Information, Communication Technologies, ICT.	Nuisance/Destruction.	Viruses and Malware.
3.	Financial, Health.	Financial profit.	Phishing and Social engineering.
4.	Public & Legal Order and Safety, Chemical and nuclear industry.	War/Defence.	Man in the middle attack, DDoS (Distributed Denial of Service), brute force attack.
5.	Space and Research.	Espionage.	Man in the middle attack.
6.	Civil administration.	Revenge.	Brute force attack, Viruses, Malware and, Phishing.

2.4. Security countermeasures in critical infrastructure.

By determining potential attacks based on attacker motivations linked to specific CI, it is possible to define the required security controls and countermeasures needed for specific infrastructure. Furthermore, linking the above factors creates an overall view of the best CI security practices. For example, the Saudi national cybersecurity authority defined four domains for the security controls Governance, Defence, Resilience and Cloud Computing, as shown in Figure 1 [13].

Figure 1. The relations between all cybersecurity domains.

Recent literature offers similar findings on the importance of security controls and countermeasures against attack methods, as shown in Table 3 [14]–[16].

Table 3. Security controls and countermeasures facing possible attack methods [13]

No.	Security controls and countermeasures.	Possible attack methods
1.	Maintaining & updating critical systems and patches.	Malware and Software vulnerability attacks
2.	Denying remote access from outside the country.	Man in the middle attacks.
3.	Implementing multi-factor authentication for all users and privileged users.	Phishing, social engineering and password brute-force attacks.
4.	Developing and applying a high-standard and secure password policy.	Unauthorized access and password brute-force attacks.
5.	Managing service accounts for applications and systems and disabling interactive login from these accounts.	Unauthorized escalation of privilege attack
6.	Preventing direct access and modification for databases except for administrators.	SQL Injection attacks
7.	Reviewing user identities and access rights to critical applications and systems.	There are different methods such as Man in the middle, TCP SYN, ICMP flood, Smurf IP and Ping of Death attacks.

3. The PCCI approach: conceivable implementation and discussion.

By merging the four factors – CI, motivations, cyberattacks methods and security countermeasures – the PCCI approach to predicting cyber-attacks against CI can be shaped. Taking these four factors into account in sequence significantly contributes to the prediction of security risks facing CI. Therefore, the first step of the proposed approach is to understand the nature of the infrastructure, its design, its hardware and software components and its services. This understanding provides a perception of the potential risks the CI infrastructure faces. Thus, cybersecurity practitioners can predict the attack motivations, which, in turn, contributes to the understanding of potential attack methods and the tools that attackers may use. The type of infrastructure and the services it provides are closely related to the different attack motivations: political, economic, military, espionage or financial. Following this comprehensive assessment, security countermeasures will be efficient and effective.

For example, in attacks on a country's vital security infrastructure, attacker methods vary between espionage, jamming and sabotage, and these types of cyber-attack have their own advanced tools. Therefore, security practitioners in this sector must adopt security countermeasures that prevent, detect and deter these types of attacks. In the banking sector, understanding the services provided by financial institutions and banks provokes the attacker to embezzle funds and harm the owners of capital and their businesses. The following points summarise the required steps of the PCCI approach, and Figure 2 depicts the components of the PCCI in sequence.

- **Step 1:** Identify CI functionality, including the service provided by the infrastructure and the hardware and software components of the system used.
- **Step 2:** Determine the motivations behind the attack – there may be more than one motivation at the same time, the degree of motivation may vary, and motivations could be direct or indirect.
- **Step 3:** Link steps 1 and 2 so that cybersecurity practitioners help to predict potential cyber-attacks according to target and motivations.

- **Step 4:** Apply the necessary security measures to counter cyber-attacks as a proactive security action. This proposed approach in its initial form can be taken further by strengthening the knowledge of documented cyber-attacks on different CI systems and classifying the attacks to develop a predictive model of cyber-attacks based on machine learning, thus making the prediction of attacks more advanced and effective. However, building large datasets and databases and revising them requires patience and cooperation between cybersecurity authorities to collect the necessary cybersecurity information. Figure 2 illustrates the implementation steps of the PCCI approach.

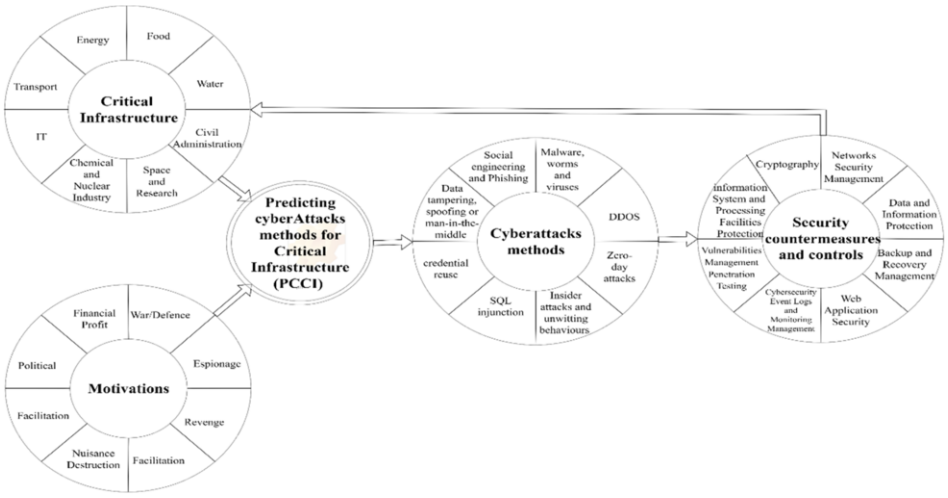

Figure 2. PCCI approach life cycle and implementation design

Many cyber-attacks have recently been reported in the war between Russia and Ukraine, and there has also been a reported ransomware attack on the Colonial Pipeline Company in the United States [9][17]; such incidents have caused massive damage to CI, and, therefore, the adoption of proactive security measures is required. Such an approach would have significantly assisted in the avoidance of these cyber-attacks, as their nature could have been predicted according to the proposed approach and would have turned security controls and countermeasures into proactive measures.

In general, applying the concept of predicting cyber-attacks on CI according to the proposed sequence starts by defining the type of CI, its design, and the services it provides, thus taking the attack motives into consideration. Further, the attack methods can be inferred from the PCCI approach. Efficient security countermeasures can therefore be adopted and applied against predicted potential cyber-attacks.

4. Conclusion

This work presents a security approach for the identification and prediction of cyber-attack methods on CI and draws the overall landscape of the necessary defence countermeasures in this field. The scientific contribution of this paper is represented by

the extraction from published studies of the framing of the influencing factors that shape the theoretical concept of PCCI, a proactive security approach through which cyber-attacks on CI can be predicted. Thus, the development of the PCCI approach will be positively reflected in the measures taken against cyber threats. The proposed PCCI approach is a security measure that predicts cyber-attacks from different perspectives based on four main factors: CI, attack motivation, attack methods and security countermeasures. Security practitioners adopting this approach will be able to significantly enhance the development of high-efficiency proactive security measures that, in turn, will play significant roles in neutralizing any damage to CI. Also, this approach can be taken further by applying artificial intelligence to threat intelligence, thereby making the prediction more comprehensive and effective.

References

[1] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for Industry 4.0 in the current literature: A reference framework," *Computers in Industry*, vol. 103, pp. 97–110, 2018, doi: 10.1016/j.compind.2018.09.004.

[2] P. Ii and A. Cisco, "Cisco. Annual cybersecurity report," 2018. https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

[3] A. I. June, "How CEOs can tackle the challenge of cybersecurity in the age of the Internet of Things How CEOs can tackle the challenge of cybersecurity in the age of the Internet of Things," no. June, 2017.

[4] R. E. Izzaty, B. Astuti, and N. Cholimah, "GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION," *Angewandte Chemie International Edition, 6(11), 951–952.*, pp. 5–24, 1967.

[5] X. Fang, M. Xu, S. Xu, and P. Zhao, "A deep learning framework for predicting cyber attacks rates," *Eurasip Journal on Information Security*, vol. 2019, no. 1, 2019, doi: 10.1186/s13635-019-0090-6.

[6] J. Andress and S. Winterfeld, *Cyber Warfare*. Elsevier, 2014. doi: 10.1016/C2013-0-00059-X.

[7] T. J. Holt, J. D. Freilich, and S. M. Chermak, "Exploring the Subculture of Ideologically Motivated Cyber-Attackers," *Journal of Contemporary Criminal Justice*, vol. 33, no. 3, pp. 212–233, 2017, doi: 10.1177/1043986217699100.

[8] M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of attack projection, prediction, and forecasting in cyber security," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 640–660, 2019, doi: 10.1109/COMST.2018.2871866.

[9] K. J. Dill, "The Cyber Defense Review m RESEARCH NOTES m," *The Cyber Defense Review*, vol. 4, no. 1, pp. 125–136, 2019, [Online]. Available: https://www-jstor-org.eserv.uum.edu.my/stable/pdf/26267358.pdf

[10] M. Rounds and N. Pendgraft, "Diversity in network attacker motivation: A literature review," *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, vol. 3, pp. 319–323, 2009, doi: 10.1109/CSE.2009.178.

[11] S. Chng, H. Y. Lu, A. Kumar, and D. Yau, "Hacker types, motivations and strategies: A comprehensive framework," *Computers in Human Behavior Reports*, vol. 5, p. 100167, 2022, doi: 10.1016/j.chbr.2022.100167.

[12] M. Rounds and N. Pendgraft, "Diversity in network attacker motivation: A literature review," *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, vol. 3, pp. 319–323, 2009, doi: 10.1109/CSE.2009.178.

[13] Saudi NCA, "Critical Systems Cybersecurity Controls (CSCC – 1 : 2019)," vol. 2019, 2019.

[14] A. Bendovschi, "Cyber-Attacks – Trends , Patterns and Security Countermeasures," *Procedia Economics and Finance*, vol. 28, no. April, pp. 24–31, 2015, doi: 10.1016/S2212-5671(15)01077-1.

[15] C. Islands, "Research Article Protecting 'Cybersecurity & Resiliency' of Nation ' S Critical Infrastructure -," 2018.

[16] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures," *Proceedings - 2018 IEEE Global Conference on Wireless Computing and Networking, GCWCN 2018*, pp. 124–130, 2019, doi: 10.1109/GCWCN.2018.8668630.

[17] S. Corbet and J. W. Goodell, "The reputational contagion effects of ransomware attacks," *Finance Research Letters*, no. October 2021, p. 102715, 2022, doi: 10.1016/j.frl.2022.102715.