A Holistic Approach for Enhancing Critical Infrastructure Protection: Research Agenda

Livinus Obiora Nweke[1] and Stephen D. Wolthusen[1,2]

[1] Information Security and Communication Technology
Norwegian University of Science and Technology (NTNU)
Gjøvik, Norway
[2] School of Mathematics and Information Security
Royal Holloway, University of London
Egham, United Kingdom

Abstract. Critical infrastructure is an asset or a system that is essential for the maintenance of vital societal functions. The protection of such an infrastructure requires more than a technical understanding of the underlying issues; it also needs an understanding of the organisational aspects. Although there are several standards and guidelines for the protection of critical infrastructure, they are usually vague and do not offer practical solutions. In this paper, we describe a 'work in progress' holistic approach for enhancing critical infrastructure protection. First, we introduce the theoretical background of this study. Then, based on this theoretical foundation, we propose a holistic approach which takes into account both organisational and technical measures. In addition, we provide a synopsis of our research outcomes so far and our ongoing work towards enhancing critical infrastructure protection.

Keywords: Critical infrastructure protection, NIS Directive, Holistic approach

1 Introduction

There has been an increasing capability and intent to attack critical infrastructure. This is apparent from the growing number of reported attacks against critical infrastructure in the last few years. For example, it was recently reported that a ransomware attack was targeted at a critical infrastructure belonging to a United States (US) based natural-gas compression facility [13]. The situation is further exacerbated by state actors that have enormous resources for staging similar or more complex attacks. All these calls for rethinking about how we protect critical infrastructure considering the devastating effect a successful attack would have on the society.

Many efforts have been made around the world to address critical infrastructure protection (CIP). According to the European Commission, CIP can be defined as "*the ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction*" [4]. To support efforts in that direction, the Commission launched the European Programme for Critical Infrastructure Protection (EPCIP) [5]. Similar efforts have been made in North America with the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) program [16]. Even though the NERC-CIP mainly focuses on electric power, it demonstrates the importance of having a framework for the protection of critical infrastructure. Further, there is a consensus among all these efforts about the need for a holistic approach to enhancing CIP.

Several works in the literature have proposed a holistic approach for enhancing CIP [11, 12, 27]. The authors in [27] evaluate the risk assessment phase of critical infrastructure and propose an enhancement to the traditional risk management methods. They employ the cybernetic construct of the viable system model towards a holistic view of the risks against critical infrastructure. The holistic approach in [12] is concerned with critical infrastructure dependencies and draws on the results of a survey of critical infrastructure experts from several countries. Also, a holistic framework for building critical infrastructure resilience is presented in [11]. It consists of three parts: a set of resilience policies; an influence table that assesses the impact of policies on prevention, absorption and recovery stages; and an implementation methodology that defines the temporal order in which the policies should be implemented.

Unlike the works in the preceding paragraph, this study proposes a holistic approach for enhancing CIP which examines both organisational and technical measures. First, we introduce the theoretical background of this study. Then, based on this theoretical foundation, a holistic approach which consists of three parts is proposed. The first part considers policies, processes and procedures relating to CIP; the second part investigates the vulnerabilities, threats and attacks that the critical infrastructure may be exposed to; while the third part deals with prevention, detection and mitigation. Lastly, we provide a synopsis of our research outcomes so far and our ongoing work towards enhancing CIP.

The rest of this paper is organised as follows. Section 2 presents the theoretical foundation of this study and concepts related to enhancing CIP. Section 3 describes the proposed holistic approach for enhancing CIP. Section 4 provides a discussion of our research outcomes thus far and our ongoing work towards enhancing CIP. Section 5 concludes the paper.

2 Background

Critical infrastructure is an asset or a system that is essential for the maintenance of vital societal functions. The protection of such an infrastructure has become a major concern for countries around the world. This is because any successful attack against a critical infrastructure would have a devastating effect on the society. For example, the successful attack against a power transmission station, north of the city of Kiev, Ukraine, blacked out a portion of the Ukrainian capital equivalent to a fifth of its total power capacity [9]. Consequently, to protect the individual Member States and the Union as a whole against similar occurrence, the European Union (EU) enacted the Network and Information Systems (NIS) Directive [7]. Even though we use the NIS Directive in this study as the theoretical foundation, a similar approach has been introduced in the US with the creation of NIST (National Institute of Standards and Technology) framework for improving critical infrastructure cybersecurity [15].

The NIS Directive is the first EU-wide legislation on cybersecurity that came into effect November 2018. It was designed to facilitate a high common level of protection for network and information systems across the EU's critical infrastructure. The NIS Directive aims to achieve this by focusing on three top-level objectives: enhanced cybersecurity capabilities across the EU Member States, increased level of cooperation between the EU Member States and supervision of critical sectors. Also, there are two types of organizations that the NIS Directive is applicable to. They are the digital service providers and the operators of essential services (operators of critical infrastructure). However, this study focuses on the requirements of NIS Directive that applies to the operators of critical infrastructure.

Critical infrastructure operators are obliged by the NIS Directive to ensure the protection of their network and information systems. The NIS Directive clearly states that the "*responsibilities in ensuring the security of network and information systems lie, to a great extent, with operators of essential services*". It went further to encourage a culture of risk management, which involves risk assessment and the implementation of appropriate security measures [7]. These measures are to include measures to identify any risks of incidents through the understanding of vulnerabilities, threats and attacks, and countermeasures to prevent, detect and mitigate their impact.

Furthermore, the NIS Directive observes that the "*technical and organisational measures imposed on the operators of essential services and digital service providers should not require a particular commercial information and communications technology product to be designed, developed or manufactured in a particular manner*". This implies that critical infrastructure operators have the liberty to adopt any type of technical and organisational measures towards enhancing the protection of critical infrastructure. Although hardware manufacturers and software developers are not classified as critical infrastructure by the NIS Directive, it notes that their products enhance the protection of network and information systems within the critical infrastructure. Thus, they have an essential role in supporting critical infrastructure operators in order to protect their network and information systems.

Based on the above theoretical background, we propose a holistic approach for enhancing CIP in Section 3. This holistic approach draws from our experience in our ongoing research towards enhancing CIP. Similar to the suggestions made in the NIS Directive, we note that a holistic approach to enhancing CIP should not only include technical measures, but also, should consider organizational measures which cover policies, processes and procedures. In addition, we provide a synopsis of our research outcomes so far and our ongoing work towards enhancing CIP in Section 4.

3 The Holistic Approach

In this study, we propose a holistic approach for enhancing CIP which consists of three parts. The first part considers policies, processes and procedures relating to CIP. In the second part, the concern is to understand the vulnerabilities, threats and attacks that the critical infrastructure may be exposed to. And the third part of the holistic approach deals with prevention, detection and mitigation of the vulnerabilities, threats and attacks that have been identified in the second part of the holistic approach. Whilst the first part deals with the organisational measures of CIP, the second and the third parts are mainly concerned with the technical measures related to CIP. This holistic approach can be viewed as a triangular framework as shown in figure 1.

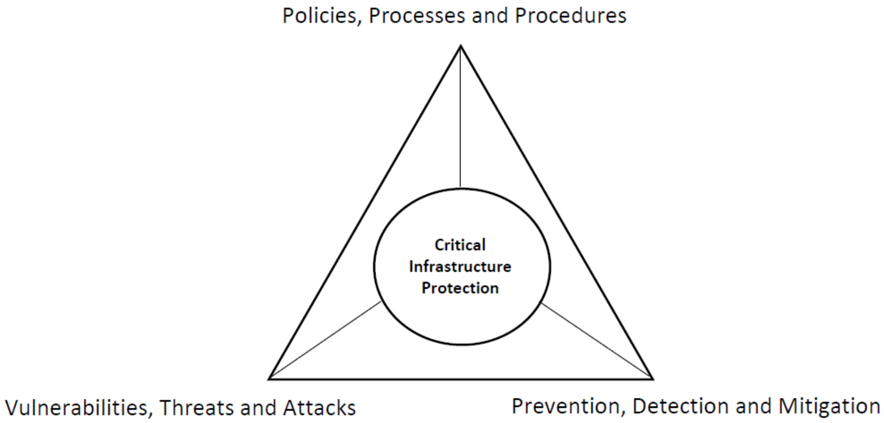
Policies, Processes and Procedures
Critical Infrastructure Protection
Vulnerabilities, Threats and Attacks
Prevention, Detection and Mitigation

Fig. 1: The Holistic Approach

3.1 Policies, Processes and Procedures

Policies refer to rules, laws, regulations, or set of guidelines. They provide guidelines for the implementation of processes and procedures. With regards to enhancing CIP, we can define policies as rules, laws, regulations, or set of guidelines that are related to CIP, which are established to guide the activities of critical infrastructure operators. Considering the importance of critical infrastructure, these policies are usually enacted at the national and international levels. For example, in the EU, either directive or regulation could be used. When a directive is issued, the individual Member States are required to enact laws using the directive as the minimum standard and in the case of a regulation, it is usually binding for all Member States [6].

Processes can be defined as steps that must be taken to ensure compliance with a policy. An understanding of processes is an essential prerequisite for complying with the defined policies. Processes usually include specifying who is responsible for executing a task, what task should be performed, and when that task should be performed. For instance, given a critical infrastructure operator like the healthcare providers, processes are high set of things defined by the providers in order to ensure compliance with policies defined at the national and international levels.

Procedures are specific, detailed series of actions that must be performed and are geared towards implementing a process and complying with a policy. In the context of CIP, procedures are related to individuals involved in the actual operations within the critical infrastructure. They are the practical application of the processes and policies defined at the national or international levels, and management level of the critical infrastructure operations respectively. For example, in the healthcare sector, an understanding of procedures for enhancing CIP may require the modelling and analysis of healthcare professionals' security practices.

In general, policies, processes and procedures are related to the activities of humans involved in the protection of critical infrastructure. There is a consensus among security practitioners that humans are usually the weakest link in the security chain. Hence, technical measures alone are not enough for enhancing CIP. It is also important that there is a clear understanding of policies, processes and procedures among all those responsible for protecting critical infrastructure. This will ensure that with strong technical measures in place, the organisational measures are also strengthened.

3.2 Vulnerabilities, Threats and Attacks

Vulnerabilities are weaknesses in a system that can be exploited to wreak havoc on the system. These vulnerabilities could exist not only in the technology being used, but also in the configurations and the implemented security policies [28]. In the critical infrastructure sector, several technologies are used to support its operations, and an understanding of the vulnerabilities in such technologies is an essential step for enhancing their protection. For example, vulnerability discovery models have been used in the literature for predicting future software vulnerabilities based on their historical behaviour [2, 10]. It is possible to use a similar approach to understanding and predicting future vulnerabilities of systems deployed for CIP.

Threats can be viewed as events that are likely to cause harm to the confidentiality, integrity or availability (CIA model [17]) of systems, through unauthorized disclosure, misuse, alteration or destruction [14]. They can be malicious or accidental. Malicious threats are those actions that could exploit the vulnerabilities in a system to cause harm to the system while accidental threats are those unintended insider actions that could cause harm to the system. The process of understanding the likelihood of those threats being realized is called threat modelling. Threat modelling approaches have been employed for enhancing CIP [1, 3, 25]. However, we have observed that the regular threat modelling approaches are not able to adequately capture the threats to cyber-physical system (CPS) which is a major part of critical infrastructure, due to timing, uncertainty and dependencies that exist between its entities [20]. Therefore, there is a need for an appropriate threat modelling approach that takes into account the unique features of CPS.

Attacks are actions that leverage one or more vulnerabilities to realize a threat. They are usually intentional acts aimed at causing damage to a system. Like other information systems, attacks against critical infrastructure can be classified according to the CIA model. The most severe type of attack for critical infrastructure is the attack that affects availability. A critical infrastructure is required to be available all the time, even in the face of a natural disaster. This makes attacks against the availability of a critical infrastructure like the denial of service (DoS) attack as one of the most extreme types of attack that needs to be considered for enhancing CIP.

Undeniably, enhancing CIP requires a good understanding of vulnerabilities, threats and attacks. As one of the technical measures in our proposed holistic approach, this understanding will provide practitioners with a tool for predicting future vulnerabilities of systems deployed for CIP, better threat modelling approach to adequately capture the threats to critical infrastructure and a good insight into the possible attacks against critical infrastructure. All these will provide the necessary knowledge needed for the third part of our proposed holistic approach which involves prevention, detection and mitigation.

3.3 Prevention, Detection and Mitigation

Prevention refers to actions that could stop attacks against a system from happening. It requires an understanding of all possible attacks that could be targeted against a system and then implementing appropriate measures to prevent them from occurring in the first place. For example, in CIP, a possible approach for preventing attacks against availability may involve the use of redundant systems. Here, two or more systems may be used to provide the same service such that if one of the systems fails, another system continues to provide the same service without any interruptions.

Detection is the process of uncovering attacks against a system. The overall goal of detection mechanisms is to be able to identify attacks and to implement appropriate countermeasures for minimising the impact of those attacks. With regards to CIP, there is an increasing complexity in the types of reported attacks. Thus, the use of traditional detection mechanisms like the intrusion detection systems no longer suffices for the protection critical infrastructure. There is a need for detection mechanisms that combine more than one approach for enhancing CIP.

Mitigation is concerned with minimising the severity of attacks against a system. It requires an understanding of when the system is under attack. This implies that the mitigation process is activated after the detection process has occurred. The mitigation strategies that should be implemented for a system depend on the functionality and the services provided by the system. For critical infrastructure, service availability is usually a priority. It follows that the mitigation strategies for critical infrastructure should ensure the availability of service even in the midst of an attack or a restoration of service as quickly as possible.

In summary, a good grasp of the prevention, detection and mitigation techniques is essential for enhancing CIP. The prevention process allows practitioners to implement the required technical measures for ensuring that attacks against critical infrastructure never occur. However, the attack landscape is constantly evolving, and this makes it impossible for practitioners to implement all the necessary measures for preventing future attacks. Hence, detection mechanism is required to uncover when those attacks occur. With the detection of the attacks, countermeasures are needed to minimise the impact of those attacks. These countermeasures are implemented using the mitigation process. Therefore, a holistic approach to enhancing CIP is one that employs appropriate technical measures in addition to robust organisational measures which cover policies, processes and procedures implemented towards enhancing the protection of critical infrastructure.

4 Discussion

Already, we have observed that organisational measures are very essential for enhancing CIP. To this end, we studied the legal issues related to cyber threat information (CTI) sharing among private entities for CIP in [19]. This is because CTI sharing has been proposed as an efficient and effective method for improving CIP. The work provides guidance and incentives for private entities willing to participate in CTI sharing, especially for CIP. Also, it has been observed in [8] that practising law involves anticipating how and what a judge might decide when presented with an issue, but ethics appears as a superior and stable reference to which laws can refer to. Thus, we presented in [21] the ethical implications of security vulnerability research for CIP. The result of this study shows that a security researcher could rely on the three different normative ethical frameworks to reason about the best course of action during security vulnerability research for CIP.

Furthermore, other works until now that have considered organisational measures related to CIP are presented in [24, 29]. There has been an increasing deployment of attribute-based access control (ABAC) in the healthcare sector, which is one of the sectors classified as critical infrastructure. This motivates our paper in [24] where we examined the existing literature on the application of ABAC in the healthcare sector. The work can serve as a basis for selecting and further advancing the use of ABAC in e-health systems. We also conducted a systematic literature review of artificial intelligence strategies and their hybrid aspects in [29]. The study identified appropriate artificial intelligence strategies and their hybrid aspects which can be employed to efficiently detect anomaly and malicious events in healthcare staff's security practices using the access logs.

Technical measures are the core aspects of the holistic approach and as such, they were divided into two parts. Considering the part which examines vulnerabilities, threats and attacks, we proposed a vulnerability discovery modelling with vulnerability severity in [26]. As we have already noted from the NIS Directive, hardware and software products enhance the protection of critical infrastructure. Hence, the ability to predict the future vulnerabilities of software deployed in critical infrastructure will ensure that appropriate resources are allocated for their protection. It is possible to use our proposed approach for predicting the future vulnerabilities of software deployed in critical infrastructure. We also conducted a review of asset-centric threat modelling approaches in [20]. The study observed that the existing threat modelling approaches are not able to capture all the threats to a CPS, which is one of the main components of critical infrastructure. This is because of the uncertainty, timing and dependencies that exist between the entities of a CPS. The main objective of the review is to serve as a foundation for determining the appropriate asset-centric threat modelling approaches that could be employed for a given scenario.

Moreover, our research outcomes which can be categorized into the second part of the holistic approach are published in [18, 22, 23]. We remarked in [23] that software-defined networks (SDN) are widely being adopted and are likely to be deployed in critical infrastructure. However, there is a need to evaluate the security and performance guarantees that can be given for the data plane of such critical systems. To this end, we studied the existing literature on the analysis of SDN using queueing networks and proposed ways in which models need to be extended in order to study attacks. We then employed one of the proposed models to study the effect of adversarial flow in software-defined industrial control networks using a queueing network model in [22]. This work provides useful insights for benchmarking and facilitates the identification of factors that could cause the network to breach the stringent QoS requirements in software-defined industrial control networks. In addition, we noted in [18] that real-time communication protocols are among the most commonly used communication protocols in critical infrastructure and they are used to monitor and control industrial automation processes deployed in critical infrastructure. Thus, we proposed an adversary model for attacks against these communication protocols taking into account their unique properties. This is to facilitate the understanding of how adversarial actions may influence the communication protocols deployed for CIP.

One of our ongoing work is to develop a legal compliance framework that will assist private entities within the critical infrastructure sector to share CTI among themselves for the purpose of improving their overall cyber intelligence and defence. Other ongoing work is the asset-centric threat modelling of CPS using a formal technique to address the limitations of the existing approaches identified in [20]. We are also investigating the prevention, detection and mitigation strategies (third part of the holistic approach) for the vulnerabilities, threats and attacks we have identified in the second part of the holistic approach.

5 Conclusion

Enhancing CIP requires a combination of both organisational and technical measures in order to be effective. In this paper, we have proposed a holistic approach for enhancing CIP which consists of three parts. The first part considers policies, processes and procedures relating to CIP; the second part investigates the vulnerabilities, threats and attacks that the critical infrastructure may be exposed to; while the third part deals with prevention, detection and mitigation. The holistic approach draws from the NIS Directive and our experience in the ongoing study towards enhancing CIP. Lastly, we have presented a synopsis of our research outcomes till date and our ongoing work which were grouped according to the three parts of the holistic approach.

References

1. Abomhara, M., Gerdes, M., Køien, G.M.: A stride-based threat model for telehealth systems. Norsk informasjonssikkerhetskonferanse (NISK) **8**(1), 82–96 (2015)
2. Alhazmi, O., Malaiya, Y.: Prediction capabilities of vulnerability discovery models. pp. 86–91. IEEE (2006). https://doi.org/10.1109/RAMS.2006.1677355
3. Atif, Y., Jiang, Y., Jianguo, D., Jeusfeld, M., Lindström, B., Andler, S., Brax, C., Haglund, D., Lindström, B.: Cyber-threat analysis for cyber-physical systems (2018)
4. European Commission: Green paper on a european programme for critical infrastructure protection. Tech. rep., European Commission (2005)
5. European Commission: Communication from the commission on a european programme for critical infrastructure protection. Tech. rep., European Commission (2006)
6. European Union: Regulations, directives, and other acts, https://europa.eu/european-union/eu-law/legal-acts
7. European Union: Directive (eu) 2016/1148 of the european parliament and of the councilof 6 july 2016. Official Journal of the European Union (2016)
8. Fuster, G.G., Gutwirth, S.: Ethics, law and privacy: Disentangling law from ethics in privacy discourse. In: Proc. Technology and Engineering 2014 IEEE Int. Symp. Ethics in Science. pp. 1–6 (May 2014)
9. Greenberg, A.: 'crash override': The malware that took down a power grid (2017), https://www.wired.com/story/crash-override-malware/
10. Joh, H., Kim, J., Malaiya, Y.K.: Vulnerability discovery modeling using weibull distribution. pp. 299–300. IEEE (2008). https://doi.org/10.1109/ISSRE.2008.32
11. Labaka, L., Hernantes, J., Sarriegi, J.M.: A holistic framework for building critical infrastructure resilience **103**, 21–33 (2016)
12. Laugé, A., Hernantes, J., Sarriegi, J.M.: Critical infrastructure dependencies: A holistic, dynamic and quantitative approach. Int. J. Crit. Infrastructure Prot. **8**, 16–23 (2015)
13. Mühlberg, B.: U.s. critical infrastructure victim of ransomware attack (Mar 2020), https://www.cpomagazine.com/cyber-security/u-s-critical-infrastructure-victim-of-ransomware-attack/
14. National Institute of Standards and Technology: Information security: Guide for conducting risk assessments (Sep 2012)

15. National Institute of Standards and Technology: Framework for improving critical infrastructure cybersecurity. Tech. rep., National Institute of Standards and Technology (2014)
16. NERC: Critical infrastructure protection (cip) standards. Tech. rep., North American Electric Reliability Corporation (2020)
17. Nweke, L.O.: Using the cia and aaa models to explain cybersecurity activities. PM World Journal **6** (2017)
18. Nweke, L.O., Weldehawaryat, G.K., Wolthusen, S.D.: Adversary model for attacks against iec 61850 real-time communication protocols. In: 16th International Conference on the Design of Reliable Communication Networks DRCN. pp. 1–8. IEEE (2020)
19. Nweke, L.O., Wolthusen, S.: Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection. NATO CCDCOE 12th International Conference on Cyber Conflict (2020)
20. Nweke, L.O., Wolthusen, S.: A review of asset-centric threat modelling approaches. International Journal of Advanced Computer Science and Applications **11**(2), 1–6 (2020)
21. Nweke, L.O., Wolthusen, S.D.: Ethical implications of security vulnerability research for critical infrastructure protection. 15th International Conference on Wirtschaftsinformatik (2020)
22. Nweke, L.O., Wolthusen, S.D.: Modelling adversarial flow in software-defined industrial control networks using a queueing network model. In: IEEE Conference on Communications and Network Security (2020)
23. Nweke, L.O., Wolthusen, S.D.: Resilience analysis of software-defined networks using queueing networks. In: 2020 International Conference on Computing, Networking and Communications (ICNC). pp. 536–542. IEEE (2020)
24. Nweke, L.O., Yeng, P., Wolthusen, S.D., Yang, B.: Understanding attribute-based access control for modelling and analysing healthcare professionals' security practices. International Journal of Advanced Computer Science and Applications **11**(2), 683–690 (2020). https://doi.org/10.14569/ijacsa.2020.0110286
25. Rekik, M., Gransart, C., Berbineau, M.: Cyber-physical threats and vulnerabilities analysis for train control and monitoring systems. In: Proc. Computers and Communications (ISNCC) 2018 Int. Symp. Networks. pp. 1–6 (Jun 2018)
26. Shukla, A., Katt, B., Nweke, L.O.: Vulnerability discovery modelling with vulnerability severity. In: 2019 IEEE Conference on Information and Communication Technology. pp. 1–6. IEEE (2019). https://doi.org/10.1109/CICT48419.2019.9066187
27. Spyridopoulos, T., Topa, I., Tryfonas, T., Karyda, M.: A holistic approach for cyber assurance of critical infrastructure with the viable system model. In: Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Kalam, A.A.E., Sans, T. (eds.) ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings. IFIP Advances in Information and Communication Technology, vol. 428, pp. 438–445. Springer (2014)
28. Whitaker, A., Newman, D.P.: Penetration Testing and Network Defense. Cisco Press (2006)
29. Yeng, P.K., Nweke, L.O., Woldaregay, A.Z., Yang, B., Snekkenes, E.A.: Data-driven and artificial intelligence (ai) approach for modelling and analyzing healthcare security practice: A systematic review. In: Intelligent Systems Conference (IntelliSys) 2020 (2020)