Cyber Warfare and Cyber Terrorism Threats Targeting Critical Infrastructure: A HCPS-based Threat Modelling Intelligence Framework

Rennie Naidoo and Carla Jacobs
University of Pretoria, Pretoria, South Africa

rennie.naidoo@up.ac.za
u17053422@tuks.co.za

Abstract: Acts of cyber warfare and cyber terrorism (CWCT) that target a nation's critical infrastructure (CI) are quickly becoming a larger threat to national security than conventional kinetic warfare strategies. Adversaries or potential adversaries can target a nation's electrical grids, telecommunications, financial services, transportation, healthcare systems, and other forms of CI. These acts pose a major threat to a nation's CI and consequently exposes citizens to public health, safety, security, and economic development risks. Identifying cyber vulnerabilities and threats can help nations to improve their CI defence strategies. There is a crucial need for research that can aid in understanding the major types of CI threats and by what method they might occur. This paper conducts a systematic literature review to develop an initial threat intelligence framework of CWCT attacks on CI. Drawing from a Human–Cyber–Physical Systems (HCPS) lens, the threat intelligence framework classifies CWCT attacks according to the methods, weapons, vulnerabilities, targets and impact of the CWCT attack. The cyber warfare community can extend the proposed HCPS-based threat intelligence framework to develop more advanced cyber security mitigation strategies, training scenarios and simulations. Large-scale monitoring of CI threats requires in-depth threat intelligence analysis and a collaborative defence strategy. This calls for a higher degree of coordination and orchestration between the military, intelligence agencies, government departments, multinational allies, regulators, and commercial entities. Future research can customize the proposed HCPS-based threat intelligence framework to cater for the unique threats facing specific CI domains.

Keywords: Cyberwar; Cyber Terrorism; Human–Cyber–Physical Systems; Threat Modelling; Critical Infrastructure; Systematic Literature Review

1. Introduction

Cyberwarfare has become a major concern for many nations and is considered a significantly higher threat to national security than conventional kinetic warfare strategies (Kaiser, 2014). A recent global survey found that cyberattacks targeting critical infrastructure made up 40% of all nation-state attacks (Microsoft's Digital Defense Report, 2022). While a substantial portion of this share was made up of Russian state-sponsored cyberattacks targeting Ukrainian infrastructure in the ongoing Russian-Ukrainian war, some scholars argue that any cyberattack aimed at destroying CI systems is tantamount to a declaration of war (Indrajit et al, 2021). Cyberattacks poses a major threat to a country's electrical grid, telecommunications, financial services, transportation and healthcare systems. The impact of these attacks often extend beyond the targeted CI with the potential of causing significant collateral damage (Abouzakhar et al, 2018).

Many nations are now identifying threats and mitigation strategies that will enable them to better protect their CI from the attacks of adversaries or potential adversaries in cyberspace. Recently, President Biden enacted the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA, 2022) which reinforces the need to improve the threat modelling and intelligence capability of US-based organizations and EU allies. Given the increasing volume and diversity of threats targeting CI, spotting trends and quickly sharing intelligence is crucial for hardening and defending CI. A nation's threat modelling and intelligence capability can improve the safeguarding of CI by developing and strengthening their cyber capabilities and tactics.

According to Shi et al (2021), threat modelling is a systematic process for identifying, evaluating and developing countermeasures to protect critical assets from threats and threat actors. A crucial extension of threat modelling is cyber threat intelligence (Kotsias et al, 2022; Tounsi and Rais, 2018; Shackleford, 2017). Cyber threat intelligence refers to the process of "acquiring, processing, analysing, and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities inside the cyber domain to offer courses of action that enhance decision making" (Ettinger, 2019). A number of threat models exist, such as STRIDE, DREAD, P.A.S.T.A, Trike, VAST, Attack Tree, Common Vulnerability Scoring System (CVSS), T-MAP and OCTAVE, to assist in identifying vulnerabilities and mitigating potential threats facing networks, computers, software products, and data (Shostack, 2014, Kotsias et al, 2022; Shi et al, 2021). However, these models for the most part focus at an organizational level. More recently, the Cyber-Physical Systems (CPSs) approach has been proposed for threat

modelling and analysis of specific CI domains (Ding et al, 2017; Lee 2015). However, these approaches tend to emphasise computational and the physical components without explicitly integrating the human component into their models which may be too narrow for the holistic analysis of CWCT attacks targeting national CI domains (Xiong and Lagerström, 2019).

This research paper draws from recent research on Human–Cyber–Physical Systems (HCPSs) to provide an initial threat intelligence framework that identifies the different types of cyber warfare and cyber terrorism (CWCT) attacks on CI across the globe (Zhou et al, 2019). The research surveys recent literature to analyse the different types of attacks that have been observed in recent years with the aim of classifying them according to distinct factors such as method, weapons, vulnerabilities, and targets of the CWCT attack. The study also briefly discusses some of the methods and tactics that can be adopted by cybersecurity practitioners to harden CI.

The rest of the paper is organized as follows: first, we outline the HCPS-based framework as a basis for our analysis. Second, we present our systematic literature approach to review the selected CI literature in more detail. We then present and discuss the results and finally conclude the paper.

2. Conceptual Foundations

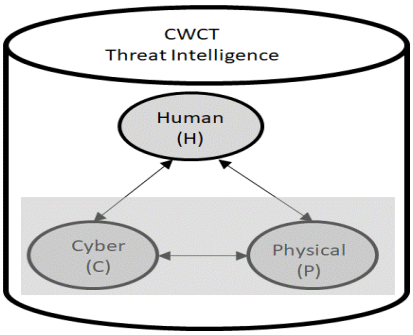

Figure 1: HCPS-based threat intelligence modelling framework

A popular way to think about CI cybersecurity is to view it as a cyber-physical system (CPS). While CPS is sometimes conflated with the term cybersecurity, CPS is more encompassing as it entails all interactions between the cyber and physical environment. The architecture of a cyber-physical systems (CPS) includes digital, analogue and physical components (Lee 2015). From an intellectual standpoint, the dominant approaches to study CPS is multidisciplinary but tends to be limited to the computer science and the engineering disciplines. CPS has been valuable to the study of the cybersecurity of CIs as it considers the dynamic interaction among computers, networking, and physical systems domains (Ding et al, 2017). However our study is aligned to more recent advances in CPS studies that are now explicitly featuring humans and human systems in the so-called Human–Cyber–Physical Systems (HCPSs) (Zhou et al, 2019). We propose a HCPS-based approach to frame threat modelling and intelligence of CWCT that target a nation's CI. To cater for the CI environment, we employ the term threat intelligence more broadly as the use of sensitising concepts to aid in thinking, learning and disseminating information about cybersecurity threats in HCPSs. Given the inherent complexity of HCPS landscape, we limit our scope to an asset and attacker centric approach to threat intelligence modelling (Tounsi and Rais, 2018; Shostack, 2014). Specifically, we pay attention to the attack target, cyber weapon or method used in the attack, vulnerabilities, and impact of the attack in a HCPS.

3. Research Method

This study has been conducted using a systematic literature review research method. Articles that focused on cyberwar or cyber-attacks on CI were included. The following search string (Cyberwar OR "Cyber War") AND (Attack OR Threat) AND "Critical Infrastructure") OR (Cybersecurity OR “Cyber Security” OR “Cyber-Attack”) AND “Critical Infrastructure”). The following databases were searched using the defined search string: IEEE Xplore® Digital Library, JSTOR and Scopus. A filtering process was used to ensure that the academic journal articles included in the systematic literature review are of high quality and relevant to the research question. Articles were first identified by using the search string. Thereafter, the duplicate articles were removed, and the abstracts of the remaining articles were screened. After the abstract screening step, the full text for each article was then assessed for eligibility. The following table displays the results after each of the filtration steps as described.

Table 1: Results of the Filtering Process

Filter process steps	Results
Identify articles	405
Remove duplicates	391
Screen abstract	391
Screen full text	72
Studies included	44

During the data extraction process, the following dimensions have been extracted from each of the data sources: CWCT attack target, cyber weapon or method used in the attack, vulnerabilities, and impact of the attack. The purpose of extracting each of the abovementioned dimensions from each of the included research papers was to analyse and categorise the findings. The research papers included in the study were analysed according to which CI component was targeted by a cyber-attack, the vulnerabilities of a cyber-attack and the potential impact on humans, the environment, and the economy. The texts for each of the data sources included in the literature review were analysed to extract meaningful relationships that would aid in answering the research question. Certain limiting factors, such as secrecy and the ever-evolving nature of cyber risks, may affect the accuracy of the research findings.

4. Results

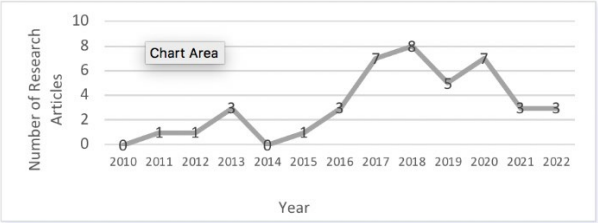

Figure 2: Cybersecurity Research Trends

Figure 2 depicts the upward trend in cybersecurity research focusing on CI components completed in the past twelve years. Although the graph is limited to the research articles included in this study, there was notable growth in cyberwar research from the year 2014 to the year 2018. To identify the components in CI that are most vulnerable to CWCT attacks, the following bar graph visually depicts in how many of the research papers each type of identified cyber-attack target was mentioned. It is important to note that some attack targets are components or systems within CIs, such as Supervisory Control and Data Acquisition (SCADA) systems, which monitors and controls Smart Grids.

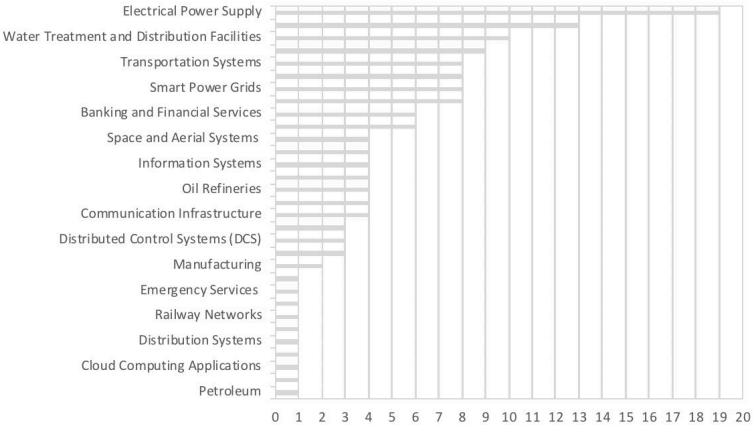

Figure 3: Critical Infrastructure CWCT Attack Targets

This literature review is directed towards identifying which types of CWCT attacks pose the biggest threat to CI. Therefore, the subsequent analysis of this research paper was completed using only the cyber-attack targets

that were mentioned in most research articles. Based on the findings depicted in the above graph, the CI systems and components of CI systems that are most vulnerable to cyber-attacks are the following: Banking and Financial Services, Cyber Physical Systems, Transportation Systems, Water Treatment and Distribution Systems, Nuclear Power Plants, Industrial Control Systems, Smart Power Grids, Supervisory Control and Data Acquisition (SCADA) Systems, Electrical Power Supply, and Hospitals and Healthcare. The identified cyber-attack weapons or methods that are used in most cyberwar attacks against the identified major targets are depicted in Figure 4.

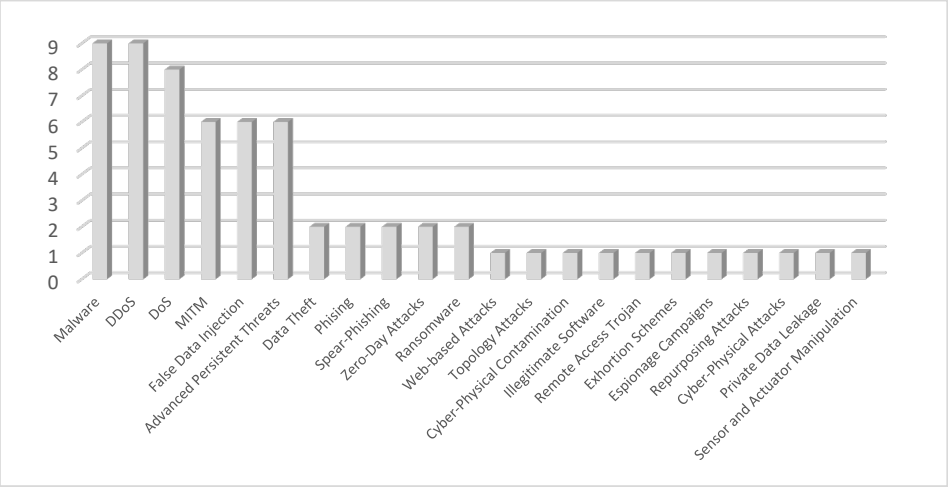

Figure 4: Cyber Weapons Mentions

The major types of cyberwar attack weapons or methods of attack are Malware, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, Man-in-the-Middle (MITM) attacks, False Data Injections (FDI) and Advanced Persistent Threats (APTs).

Figure 5 shows the identified cyber weapons used in CWCT attacks. Each attack target also highlights the impact that a potential CWCT attack could have on the normal operation of that CI component and the identified vulnerabilities which must be protected to safeguard CIs.

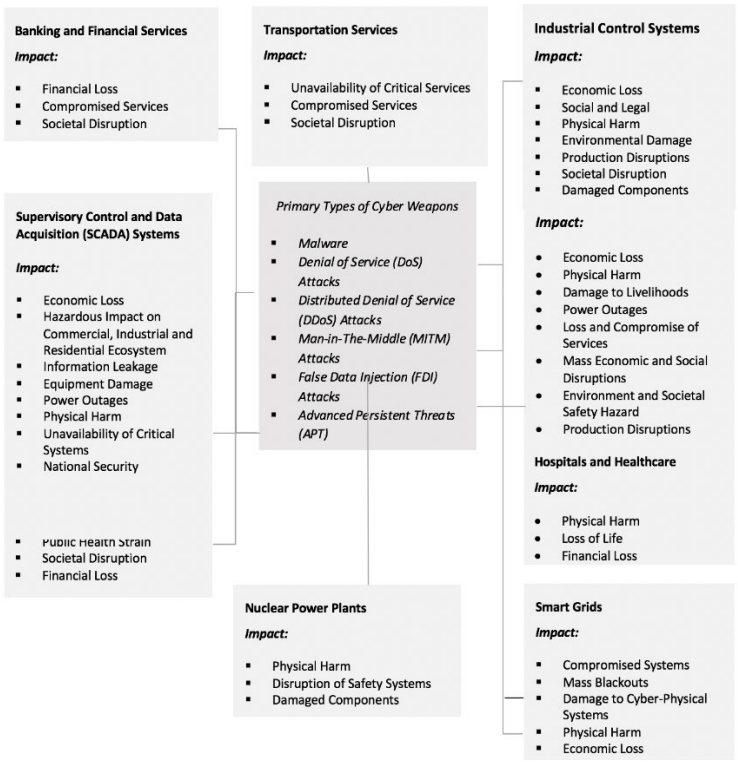

Figure 5: Impact of CWCT Cyber Threats on Critical Infrastructure

The following table contains tactics that can prevent CWCT attacks on CI from occurring or which can help to limit the amount of damage that might be caused from such an attack.

Table 2: Tactics to Address CWCT Attacks

Attack Prevention and Damage Control Tactics	References
Sensor Data Protection; Attack Detection Mechanisms; Intrusion Detection; Cryptographic Keys; Combining Cryptography and Steganography; Context-Aware Security Frameworks	*(Ashibani & Mahmoud, 2017)*
Remote Access Control Mechanisms; Data Encryption	*(Abouzakhar et al, 2018)*
Virtual Testbeds	*(Alves et al, 2016)*
Machine Learning; Artificial Intelligence	*(Nguyen et al, 2020)*
Anomaly Detection; Extended Firewall Usage; Data Leakage Protection	*(Domínguez et al, 2017)*

The main attack prevention and damage control tactics that were identified from the literature includes attack detection mechanisms, anomaly detection, data encryption, and use of cryptographic keys. Nguyen et al (2020) mentions that machine learning and artificial intelligence techniques can also be used to identify potential cyber-attacks. Multiple stakeholders including the military, intelligence agencies, government departments, multinational allies, regulators, and commercial entities will need to establish close partnerships develop the threat intelligence capability required to secure CI.

5. Discussion

The focus of this study has been on identifying the major types of cyberwar threats facing CI. Certain CI components and systems within them more important to national security than others, and greater attention must be given to ensuring the protection and functioning of these. CI such as the electrical power supply and smart power grids are the backbone of many other national CIs such as transportation systems, healthcare, and water distribution (Adepu et al, 2020). In the research findings, electrical power supply was identified as the most vulnerable CWCT attack target. This is a major challenge given that this CI is also the backbone on which many other CIs such as healthcare and banking services are entirely reliant.

The protection of cybersecurity systems in the healthcare and water distribution sector is crucial because attacks on these have serious public health consequences. Based on the findings in literature, humans can experience severe health risks or even loss of life when a country's healthcare infrastructure becomes the target of a major cyberwar attack. According to Kendzierskyj and Jahankhani (2019), there has been a significant increase in data breaches and ransomware attacks in the healthcare sector since 2016, the primary reason being that the systems are in critical need of cybersecurity enhancements. Delays or interruptions in these systems would have a major impact on healthcare operations. The major types of CWCT attacks against healthcare infrastructure that were identified from the data analysis were Denial of Service (DoS) attacks, Malware, Private Data Leakage and Data Theft. The consequences of these attacks are patients suffering physical harm and financial loss to the patients and hospitals. In some cases, attacks on hospital infrastructure were even classified as life-threatening (Abouzakhar et al, 2018). Some of the attack prevention tactics identified by Abouzakhar et al (2018) to impede Denial of Service attacks on hospitals were the implementation of effective remote access control mechanisms, proper security configuration and intrusion detection.

As identified in the findings, traditional electrical power grids and modern smart power grids are a major CI cybersecurity concern. Unlike traditional electrical power grids, communication networks play a crucial role in the smart grid environment where components such as sensors and controllers are continually communicating with and exchanging data between each other (Gupta & Akhtar, 2017). Due to the heavy interconnectivity of the components in smart power grids, they are more susceptible to cyber-attacks than the traditional manual power grids. Although their connectivity and intelligence make them an appealing target for potential CWCT attacks, it also minimises the impacts that an attack may have, because they can be reconfigured without human intervention due to their interconnected nature. This capability of the smart grid can play an important role in the prevention of negative cyber-attack outcomes, such as mass electrical outages (Gupta & Akhtar, 2017). Some extended security measures identified by Domínguez et al (2017) for the protection of smart grids and other CIs include anomaly detection, extended firewall usage, and data leakage protection.

Industrial control systems have also been identified as a major cyberwar attack target. To elaborate on one of the identified vulnerabilities in industrial control systems, Domínguez et al (2017) identified a mismatch between industrial control experts' knowledge in the field of computer and cyber security, and cybersecurity experts' knowledge of industrial control system operations. According to Domínguez et al (2017), industrial control experts generally lack computer security training and cybersecurity experts tend to disregard industrial control system operations, which leaves a concerning knowledge and skills gap that must be addressed by appropriate training environments (Domínguez et al, 2017). Another serious vulnerability can be seen for industrial control systems (ICS), which were originally designed for secluded operations. Because they were designed as isolated systems, their immersion into the world of interconnectivity exposes these systems to several alarming external cybersecurity threats that were not anticipated previously (Domínguez et al, 2017).

Supervisory Control and Data Acquisition (SCADA) systems were identified as a key component in CIs. According to Huang et al (2017), the protection of SCADA systems are a major national cybersecurity concern, as they are a crucial component of industrial applications like smart grids. SCADA systems are used in the monitoring and controlling of critical processes, and attacks against these could have numerous consequences on a country, such as power outages and information leakages. Samanti et al (2016) argues that SCADA Systems are primarily under security threats from insiders because SCADA systems and networks have largely remained isolated from the internet for most of their existence. A method to address the CWCT attacks on SCADA systems was identified by Nguyen et al (2020), which involves using machine learning and artificial intelligence techniques to identify potential cyber-attacks.

6. Conclusion

This study surveyed the major types of cyber warfare and cyber terrorism (CWCT) threats to CI by examining recent types of cyber threats that were aimed at the different types and components of national CI. This literature review built on previous research by developing an initial threat intelligence framework drawing from key features of a Human-Cyber–Physical-Systems (HCPS). This particular study identifies the different types of CWCT attacks on CI observed in recent years and classifies each of these attacks according to factors including method, weapons used, vulnerabilities, and targets of each of the CWCT attacks. Two of the CI components that were identified as having the highest risk of being targeted by CWCT attacks were the electrical power supply infrastructure and related SCADA system components. Tactics to address the threats facing CI include creating training environments to address cybersecurity knowledge gaps, implementing proper security configuration and intrusion detection methods, and using machine learning and artificial intelligence techniques to identify potential cyber-attacks. Threat mitigation also requires a high degree of coordination and orchestration between the military, intelligence agencies, government departments, multinational allies, regulators, and commercial entities. Researchers in the field of cyberwar research can expand on and customize the proposed CI CWCT threat intelligence framework to cater for the unique threats facing specific CI components. Our future work will extend the CWCT threat intelligence framework to cater for other critical elements of a HCPS.

References

Sources reviewed in the SLR

Abouzakhar, N. S., Jones, A., & Angelopoulou, O. (2018). Internet of Things Security: A Review of Risks and Threats to Healthcare Sector. *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017.* DOI: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.62

Adepu, S., Kandasamy, N. K., Zhou, J., & Mathur, A. (2020). Attacks on smart grid: power supply interruption and malicious power generation [Article]. *International Journal of Information Security*, *19*(2), 189-211.

Ahmad, R., & Yunos, Z. (2012). A dynamic cyber terrorism framework. *International Journal of Computer Science and Information Security, 10(2), 149.*

Akhtar, T., Gupta, B. B., & Yamaguchi, S. (2018, 2018). Malware propagation effects on SCADA system and smart power grid. *IEEE International Conference on Consumer Electronics (ICCE)* https://dx.doi.org/10.1109/icce.2018.8326281

Alves, T., Das, R., & Morris, T. (2016). Virtualization of industrial control system testbeds for cybersecurity. *ACM International Conference Proceeding Series*

Arnold, N. R., Mahoney, W. R., Derrick, D. C., Ligon, G. S., & Harms, M. M. (2015). Feasibility of a Cyber Attack on National Critical Infrastructure by a Non-State Violent Extremist Organization. *Journal of Information Warfare*, *14*(1), 84-100.

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions [Article]. *Computers and Security*, *68*, 81-97.

Ashrafuzzaman, M., Jamil, H., Chakhchoukh, Y., & Sheldon, F. (2018). A Best-Effort Damage Mitigation Model for Cyber-Attacks on Smart Grids. *IEEE International Conference on Computer Software & Applications.* https://dx.doi.org/10.1109/compsac.2018.10285

Axelrod, C. W. (2013). Managing the risks of cyber-physical systems. 9th Annual Conference on Long Island Systems, Applications and Technology, LISAT 2013, DOI: 10.1109/LISAT.2013.6578215

Barmin, Y., Jones, G., Moiseeva, S., & Winkelman, Z. (2011). International Arms Control and Law Enforcement in the Information Revolution An Examination of Cyber Warfare and Information Security. *Connections*, *10*(4), 73-94.

Benameur, A., Evans, N. S., & Elder, M. C. (2013). Cloud resiliency and security via diversified replica execution and monitoring. *Proceedings - 2013 6th International Symposium on Resilient Control Systems, ISRCS 2013.* DOI: 10.1109/ISRCS.2013.6623768

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey [Review]. *Computers and Security*, *89*, Article 101677.

Botes, M., & Lenzini, G. (2022). When Cryptographic Ransomware Poses Cyber Threats: Ethical Challenges and Proposed Safeguards for Cybersecurity Researchers. *Proceedings - 7th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2022*, 562-568. DOI: 10.1109/EuroSPW55150.2022.00067

Branquinho, M. A. (2018). Ransomware in industrial control systems. What comes after Wannacry and Petya global attacks? *WIT Transactions on the Built Environment, 329-334*. DOI: 10.2495/SAFE170301

Busquim e Silva, R. A., Piqueira, J. R. C., Cruz, J. J., & Marques, R. P. (2021). Cybersecurity Assessment Framework for Digital Interface Between Safety and Security at Nuclear Power Plants [Article]. *International Journal of Critical Infrastructure Protection*, *34*, Article 100453.

Chen, Z., Yan, L., He, Y., Bai, D., Liu, X., & Li, L. (2018). Reflections on the Construction of Cyber Security Range in Power Information System. *IEEE.* https://dx.doi.org/10.1109/iaeac.2018.8577685

Djenna, A., Saidouni, D. E., & Abada, W. (2020). A pragmatic cybersecurity strategies for combating IoT-cyberattacks. *International Symposium on Networks, Computers and Communications, ISNCC 2020*. DOI: 10.1109/ISNCC49221.2020.9297251

Domínguez, M., Prada, M. A., Reguera, P., Fuertes, J. J., Alonso, S., & Morán, A. (2017). Cybersecurity training in control systems using real equipment. DOI: 10.1016/j.ifacol.2017.08.2151

Eder-Neuhauser, P., Zseby, T., Fabini, J., & Vormayr, G. (2017). Cyber attack models for smart grid environments [Article]. *Sustainable Energy, Grids and Networks*, *12*, 10-29.

Gupta, B. B., & Akhtar, T. (2017). A survey on smart power grid: frameworks, tools, security issues, and solutions [Article]. *Annales des Telecommunications/Annals of Telecommunications*, *72*(9-10), 517-549.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review*, *100*(4), 817-885.

Huang, K., Zhou, C., Tian, Y.-C., Tu, W., & Peng, Y. (2017, 2017). Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks. *IEEE.* https://dx.doi.org/10.1109/atnac.2017.8215355

Huseinovic, A., Mrdovic, S., Bicakci, K., & Uludag, S. (2018). A Taxonomy of the Emerging Denial-of-Service Attacks in the Smart Grid and Countermeasures. *2018 26th Telecommunications Forum, TELFOR 2018 - Proceedings.* DOI: 10.1109/TELFOR.2018.8611847

Indrajit, R. E., Marsetio, Gultom, R., & Widodo, P. (2021). Cyber Troops: Developing Collective Abilities to Face Cyberwarfare Challenges. *IEEE.* https://dx.doi.org/10.1109/icacsis53237.2021.9631306

Jiang, Y., Jeusfeld, M., Atif, Y., Ding, J., Brax, C., & Nero, E. (2018). A Language and Repository for Cyber Security of Smart Grids. *IEEEI.* https://dx.doi.org/10.1109/edoc.2018.00029

Kaiser, R. (2015). The birth of cyberwar. *Political Geography, 46, 11-20.* https://www.researchgate.net/publication/273113188_The_birth_of_cyberwar

Kant, D., Creutzburg, R., & Johannsen, A. (2020). Investigation of risks for critical infrastructures due to the exposure of SCADA systems and industrial controls on the Internet based on the search engine Shodan. *IS and T International Symposium on Electronic Imaging Science and Technology.* DOI: 10.2352/ISSN.2470-1173.2020.3.MOBMU-253

Kendzierskyj, S., & Jahankhani, H. (2019, 2019). The Role of Blockchain in Supporting Critical National Infrastructure. *IEEE.* https://dx.doi.org/10.1109/icgs3.2019.8688026

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology*, *51*(1), 7-15.

Kobara, K. (2016). Cyber physical security for Industrial Control Systems and IoT [Article]. *IEICE Transactions on Information and Systems*, *E99D*(4), 787-795.

Kozik, R., & Choras, M. (2013). Current cyber security threats and challenges in critical infrastructures protection. *IEEE.* https://dx.doi.org/10.1109/icoia.2013.6650236

Kshetri, N., & Voas, J. (2017). Hacking Power Grids: A Current Problem [Article]. *Computer*, *50*(12), 91-95, Article 8220480.

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system [Article]. *Applied Sciences (Switzerland)*, *8*(6), Article 898.

Laszka, A., Abbas, W., Vorobeychik, Y., & Koutsoukos, X. (2017). Synergic security for smart water networks: Redundancy, diversity, and hardening. *Proceedings - 2017 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks, CySWATER 2017.* DOI: 10.1145/3055366.3055376

Libicki, M. C. (2011). Cyberwar as a Confidence Game. *Strategic Studies Quarterly, 5(1), 132–147.* http://www.jstor.org/stable/26270514

Li, F., Yan, X., Xie, Y., Sang, Z., & Yuan, X. (2019, 2019). A Review of Cyber-Attack Methods in Cyber-Physical Power System. *IEEE.* https://dx.doi.org/10.1109/apap47170.2019.9225126

Moher D, Liberati A, Tetzlaff J, Altman DG, The PRISMA Group (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLoS Med 6(7): e1000097*. doi:10.1371/journal.pmed1000097

Nguyen, T., Wang, S., Alhazmi, M., Nazemi, M., Estebsari, A., & Dehghanian, P. (2020). Electric Power Grid Resilience to Cyber Adversaries: State of the Art. *IEEE Access*, *8*, 87592-87608.

Oughton, E. J., Ralph, D., Pant, R., Leverett, E., Copic, J., Thacker, S., Dada, R., Ruffle, S., Tuveson, M., & Hall, J. W. (2019). Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks [Article]. *Risk Analysis*, *39*(9), 2012-2031.

Park, J. W., & Lee, S. J. (2019). Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants [Article]. *Nuclear Engineering and Technology*, *51*(1), 138-145.

In Boland, A., In Cherry, M. G., & In Dickson, R. (2017). Doing a systematic review: A student's guide.

Ramotsoela, T. D., Hancke, G. P., & Abu-Mahfouz, A. M. (2020). Behavioural Intrusion Detection in Water Distribution Systems Using Neural Networks [Article]. *IEEE Access*, *8*, 190403-190416.

Samanis, E., Gardiner, J., & Rashid, A. (2022). Adaptive Cyber Security for Critical Infrastructure. *IEEE.* https://dx.doi.org/10.1109/iccps54341.2022.00043

Samtani, S., Yu, S., Zhu, H., Patton, M., & Chen, H. (2016). Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques. *IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data, ISI 2016, 25-30.* DOI: 10.1109/ISI.2016.7745438

Semertzis, I., Rajkumar, V. S., Stefanov, A., Fransen, F., & Palensky, P. (2022, 2022). Quantitative Risk Assessment of Cyber Attacks on Cyber-Physical Systems using Attack Graphs. *IEEE.* https://dx.doi.org/10.1109/mscpes55116.2022.9770140

Seyam, A. R., Nassif, A. B., Nasir, Q., Al Blooshi, B., & Talib, M. A. (2021). Deep learning techniques to detect DoS attacks on industrial control systems: A systematic literature review. *ACM International Conference Proceeding Series 2021.* DOI: 10.1145/3485557.3485577

Shrestha, M., Johansen, C., Noll, J., & Roverso, D. (2020). A Methodology for Security Classification applied to Smart Grid Infrastructures [Article]. *International Journal of Critical Infrastructure Protection*, *28*, Article 100342.

Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. *International Affairs (Royal Institute of International Affairs 1944-)*, *92*(5), 1079-1105.

Van Epps, G. (2013). Common Ground Connections U.S. and NATO Engagement with Russia in the Cyber Domain. *Connections*, *12*(4), 15-50.

Vessels, L., Heffner, K., & Johnson, D. (2019). Cybersecurity risk assessment for space systems. *Proceedings - 2019 IEEE Space Computing Conference, SCC 2019, 11-19*. DOI: 10.1109/SpaceComp.2019.00006

Ghafir, I., & Prenosil, V. (2014). Advanced persistent threat attack detection: an overview. *Int J Adv Comput Netw Secur, 4(4), 5054.*

Other references

CIRCIA (2022) “Cyber Incident Reporting for Critical Infrastructure Act of 2022”, [online], https://www.cisa.gov/sites/default/files/publications/Cyber-Incident-Reporting-ForCriticalInfrastructure-Act-of2022_508.pdf (accessed on 12 January 2023).

Ding, J., Atif, Y., Andler, S. F., Lindström, B., & Jeusfeld, M. (2017). CPS-based threat modeling for critical infrastructure protection. ACM SIGMETRICS Performance Evaluation Review, 45(2), 129-132.

Ettinger, J. (2019). Cyber intelligence tradecraft report: The state of cyber intelligence practices in the United States. Retrieved from Carnegie Mellon University: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=546686 (accessed on 12 January 2023).

Kotsias, J., Ahmad, A., & Scheepers, R. (2022). Adopting and integrating cyber-threat intelligence in a commercial organisation. European Journal of Information Systems, 1-17.

Lee, E. A. (2015). The past, present and future of cyber-physical systems: A focus on models. Sensors, 15(3), 4837-4869.

Microsoft Digital Defense Report (2022). Microsoft, https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report?rtc=1. (accessed on 11 January 2023).

Shackleford, D. (2017). Cyber threat intelligence uses, successes and failures: The SANS 2017 CTI survey. SANS Institute.

Shi, Z., Graffi, K., Starobinski, D., & Matyunin, N. (2021). Threat Modeling Tools: A Taxonomy. IEEE Security & Privacy, (01), 2-13.

Shostack, A. (2014). Threat modeling: Designing for security. John Wiley & Sons.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security, 72, 212-233.

Xiong, W., & Lagerström, R. (2019). Threat modeling–A systematic literature review. Computers & security, 84, 53-69.

Zhou, J., Zhou, Y., Wang, B., & Zang, J. (2019). Human–cyber–physical systems (HCPSs) in the context of new-generation intelligent manufacturing. Engineering, 5(4), 624-636.