Cyber Kill Chain Analysis Using Artificial Intelligence

Abstract

Artificial Intelligence (AI) tools are promising multifaceted techniques for addressing the most mundane tasks for greater efficiency and high productivity. Cyber security space is one of the areas that AI is promising to revolutionize. This study will develop a conceptual and theoretical framework to support a research design that can simulate research in understanding how AI can be applied to Cyber Kill Chain phases. This study has reviewed 21 journal and conference articles mostly from IEEE Xplore database. An overview of the application of artificial intelligence (AI) in cybersecurity, particularly within the framework of the Cyber Kill Chain was provided in this study. It also emphasizes the limitations of traditional security approaches and the necessity for innovative and intelligent defense methodologies. The results of reviewing the relevant literatures discovered that the key components of cybersecurity, includes identity, asset management, automated configuration management, security control validation, governance, risk assessment, and vulnerability identification. A theoretical framework was developed which introduces the Cyber Kill Chain model with a Unified Kill Chain model to address its shortcomings. Application of AI in cybersecurity offers an optimistic solutions to address the evolving threat landscape. AI techniques, such as machine learning, anomaly detection, and behavioural analysis, have shown great potential in enhancing various aspects of cybersecurity. However, challenges related to data quality, adversarial attacks, and privacy concerns need to be addressed for successful implementation. Further research and development are crucial to fully harness the power of AI in cybersecurity and stay ahead of evolving cyber threats.

KEYWORDS: Artificial Intelligence, Cybersecurity, Cyber Kill Chain, Application

I. Introduction

The artificial intelligence (AI) is a collection of algorithms that provide solutions to a complex mundane task. These tasks include the repetitive and deep analytics. This technology is applied in all areas of endeavours: medicine, sports, cybersecurity etc. This paper examines the application of the AI in cybersecurity. Cyber security has become one of the most important issues in cyberspace [1]. “Traditional security architecture relies on the static control of security devices deployed on special platforms, such as firewalls, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs), for network security monitoring according to the pre-specified rules” [1].

However, with the emergence of new threats, this passive defence methodology is no longer useful in protecting systems against new cyber security threats, such as advanced persistent threats (APTs) and zero-day attacks. Moreover, as cyber threats become pervasive and sustainable, the diverse attack entry points, high-level intrusion mode, and systematic attack tools reduce the cost of cyber threat deployment.

"Artificial intelligence (AI) is a fast-growing branch of computer science that researches and develops theories, methods, techniques, and application systems to simulate, extend, and expand human intelligence. AI has a wide range of applications, such as facial recognition, speech recognition, and robotics, but its application scope goes far beyond the three aspects of image, voice, and behaviour. It also has many other outstanding applications in the field of cyber security, such as malware monitoring and intrusion detection" [2].

Artificial Intelligence (AI) tools are promising multifaceted techniques for addressing the most mundane tasks for greater efficiency and high productivity. This paper seeks to review how organizations can use the application of the Cyber Kill Chain and the Unified Cyber Kill methodologies to identify threat intelligence teams in analyzing attack patterns, incidence response teams using the proposed framework to investigate breaches, and implement preventive measures based on the stages of the Kill Chan.

This paper is organized as follows: section two of this paper documents related work on the key components of Cybersecurity and Cyber Kill Chain. Section three introduces the theoretical frameworks (Cyber Kill Chain and the Unified Kill Chain). Section four presents the discussions, and section five summarizes the paper and presents some thoughts on future study.

II. Literature Review

This section presents the review of related literature on the key components of Cybersecurity. The reviewed components are as follows:

1. Identify

"The identify function provides the foundation for the other cybersecurity functions by pinpointing the critical functions and risks associated with systems, people, assets, and data. This helps develop an understanding of the current state of the cybersecurity, identify gaps, and develop an appropriate risk management strategy to achieve the desired security based on the organization's own needs, risks and budget" [3].

2. Asset Management

"Asset management is the process of identifying and keeping track of the information, people, equipment, systems, and buildings that help an organization accomplish its goals and are proportionate to the asset's relative importance to those goals and risk strategies. It includes the discovering, inventorying, managing, and tracking of assets to protect them. An AI-based asset management system can solve many of these challenges by feeding new levels of intelligence to the human team across the following use cases" [4].

3. Asset Inventory Management.

Researchers have developed different approaches to asset classification using machine learning algorithms. Promyslov et al. [5] used "a k-means clustering to classify the assets according to their cybersecurity requirements based on their safety, functionality, and integrity in a nuclear power plant". Millar et al. [6] proposed "a random forest-based machine learning classifier for operating system classification and identification of the vulnerable

devices on the network". Several studies [7-8] focus "on identifying and classifying IoT devices based on their network-traffic characteristics".

4. Automated Configuration Management.

The customization of the system's configuration to ensure the required level of performance and security is important to reduce human error due to manual or sub-optimal configuration settings. Researchers [9, 10] are working "on dynamic configuration systems for online file sharing systems and distributed cloud storage based on system characteristics and operating environments using multi-objective reinforcement learning and genetic algorithms, respectively". Sharifi et al. [11] and Bringhenti et al. [12] proposed "a fully automated framework for the customization of security controls by observing the user's behaviour and by refining high-level security requirements expressed in a human-friendly language, respectively".

5. Automated Security Control Validation.

The automation of security control validation will provide the real-time monitoring of security in a changing environment and threat landscape. Researchers are working on the implementation of AI techniques for a definitive assessment of the overall security of the system using a network's telescope data [13], a building's cybersecurity framework, or by correlating the threat, vulnerabilities, and security. "This information is critical to business sustainability and serves as the basis for developing effective response and recovery strategies. AI technology can be used to automate this process" [14].

6. Automated Business Impact Analysis.

"Business impact analysis is the most important technique to determine critical functions and applications in the business environment by evaluating the impact of cybersecurity incidents on the business. Researchers are measuring the economic risk of cybersecurity in different businesses using the modelling of different known attack profiles, rare-event simulation, or by linking the business objective to the attacker's capabilities to guide a scenario analysis to determine its impact on business assets" [15].

6. Governance

"This helps to identify an organization's responsibilities and provides information about cyber risks to the management. The automatic retrieval of key risk indicators, such as the mean time between failures, the presence of unpatched systems, risk appetite or the number of attempted breaches, and converting them into knowledge, will be beneficial to prevent a cybersecurity breach by rapidly remediating the risk" [16].

7. Automated Policy Enforcement.

"Policy enforcement is crucial for organizations to ensure their compliance with the regulations and appropriate risk management. AI is being used in automated policy enforcement in traditional non-SDN networks by using a controller and policy proxies. The controller is a centralized management server used to manage software defined middleboxes

for traditional routers and a policy proxy that will identify the traffic that is subject to polices and assists it in policy enforcement" [17].

- **Risk Assessment:**
  "The manual risk assessment process is complex, costly and time consuming due to the large number of risk factors, and it requires active human involvement at every stage. The AI-based risk assessment process addresses these challenges by supporting the risk management team in the following use cases" [18].

8. Automated Vulnerability Identification & Assessment.

"An automated vulnerability assessment is the process of systematically reviewing security weaknesses in a system using automated tools for vulnerability identification, classification, exploration, and prioritization. These automated tools rely on vulnerability repositories, vendor vulnerability announcements, asset management systems, and threat intelligence feeds to identify, classify and assess the severity, and make recommendations for the remediation" [26].

- **Automated Vulnerability Detection:** These studies employ text-mining techniques to feed the machine learning based vulnerability detection models in unison with a recommendation system to help programmers to write secure code. Saha et al. [19] proposed "a new scheme for the identification of vulnerabilities across the system and network levels by modelling the behaviour of cyber-physical systems (CPS)/IoT under attack at the system and network levels and then use machine learning to discover any potential attack space".

Related Literature on Cyber Kill Chain

The study by [20] proposes a generalized solution for modelling cyberwarfare. The proposed approach is based on a five-phase method for threat analysis, which is a combination of multi objective optimization on attack tree models of the attack tree. The attack tree model consists of a swarm of adversaries and a network of attackers. The network is divided into two parts: the first part is used to identify the attackers, and the second part uses a set of attacks to detect the target behaviour. The third part of the attacks is used as a target. The fourth part uses the network to analyse the threat sources that could lead to the result of data theft.

The study by [21], presented a comprehensive analysis of the different types of malware that infiltrate businesses through the use of agent based intrusion detection systems. The malware is classified into three categories: infection, propagation, and covert attack. The classification of the malware is then performed using a set of effective analysis techniques, and the propagation behaviour is also performed. Each analyzed ransomware uses different means to execute the attributes that are common amongst them. The results of the analysis presented in the paper can be used to understand the behavior of new ransomware, in order to avoid any new attack. However, it is quite difficult to avoid zero-day attacks that exploit newly identified vulnerabilities but having the understanding of general ransomware behavior can assist analysts to stop a ransomware before it encrypts the file system.

Security Information & Event Management (SIEM) system is one of the systems that can be used to produce cyber security situational awareness (cyber SA) and detect those intrusion attempts. The objective of this study is to create a novel construct that is used in developing and managing SIEM use cases throughout its lifecycle and to help in directing the development efforts towards the most needed sections of the environment. The proposed construct and the study provided methods and tools to use in the SIEM capability development and cyber security kill chain models are utilized as part of the solution. The results of the interviews and researchers' personal experiences were used to assess the proposed solution and compare the acquired results with the objectives set for the study [22].

The study by [23], presented a novel kill chain based taxonomy of banking trojans for evolutionary computational framework for effective detection and prediction of advanced persistent threat actors. The SOC Critical Path (SCP) is a model to detect and predict advanced persistent threats. The presented tactics can be deployed by different techniques, for example, the semantic modelling of an advanced threat actor, the SOC critical path, and the kill chain. Specific sub tactics to convert hybrid data to a common data set and a new kill chain model, which is based on a kill chain method were also proposed. Additionally, future research lines mainly related to the specification of sub tactics and particular techniques were identified in the research. This future work is considered as a mandatory enhancement of the first approach to the process of detecting and neutralizing security threats.

Summary

This sub section present the summary of reviewed systems with their pros and cons.

Table 1: Summary of Literature Review

S/N	SYSTEM	PROS	CONS
1.	Identify	Provides the foundation for the other cybersecurity.	Based on the organization's own needs, risks and budget.
2.	Asset Management	Identifying and keeping track of the information, people, equipment, systems and buildings that help an organization accomplish its goals.	Proportionate to the asset's relative importance to those goals and risk strategies.
3.	Asset Inventory	Ensures complete visibility and control over all assets in an extended network	Identification and blocking of malware infected assets.
4.	Automated Configuration Management	Process for defining and maintaining the desired state of a system and	Dynamic configuration systems for online file sharing systems

		providing timely alerts for any misconfiguration.	and distributed cloud storage based on system characteristics and operating environments.
5.	Automated Security Control Validation	Providing the real-time monitoring of security in a changing environment and threat landscape.	Implementation of AI techniques for a definitive assessment of the overall security of the system using a network's telescope data.
6.	Automated Business Impact Analysis	Determination of critical functions and applications in the business environment by evaluating the impact of cybersecurity incidents on the business.	Linking the business objectives to the attacker's capabilities to guide a scenario analysis to determine its impact on business assets.
7.	Governance	Involves the policies, procedures and processes for understanding the environmental and operational requirements, and Monitoring the regulatory requirements of the organization.	Development of an early warning system to indicate risk development over time due to policyviolations, red flags or other symptoms.
8.	Risk Assessment	Identifying, estimating and prioritizing cybersecurity risks associated with operations, operational assets and individuals currently or in the near future	requires a careful analysis of threat, vulnerability and attack information to determine the extent to which cybersecurity events could adversely impact on the organization
9.	The study by [20], Modeling Attack, Defense and Threat	Generalized solution for modelling cyberwarfare.	The network is divided into two parts: the first part is

	Trees and the Cyber Kill Chain		used to identify the attackers, and the second part uses a set of attacks to detect the target behaviour.
10.	The study by [21], Ransomware Analysis using Cyber Kill Chain	Comprehensive analysis of the different types of malware that infiltrate businesses through the use of agent based intrusion detection systems.	Quite difficult to avoid zero-day attacks that exploit newly identified vulnerabilities.
11.	SIEM	One of the systems that can be used to produce cyber security situational awareness (cyber SA) and detect those intrusion attempts.	SIEM use cases throughout its lifecycle and to help in directing the development efforts towards the most needed sections of the environment.
12.	SOC Critical Path	Presented a novel kill chain based taxonomy of banking trojans for evolutionary computational framework for effective detection and prediction of advanced persistent threat actors.	Research lines related to the specification of sub tactics and particular techniques.

III. Theoretical Framework

Cyber Kill Chain

Cybersecurity is an increasingly important area of concern as our reliance on digital technologies continues to grow. From securing personal information to protecting sensitive government and business data, cybersecurity has become a crucial aspect of modern life.

"The Cyber Kill Chain (CKC) framework developed by Lockheed Martin is a widely accepted methodology for describing a cyberattack. It consists of seven stages: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives" [24].

1. **Reconnaissance:** Research, identification and selection of targets, often presented as creepers Internet sites such as conference proceedings and mailing lists for email addresses, social networks reports, or information on specific technologies. The

attackers gather data about the targets through company websites, social media handles or employee details. To counter this, organizations can educate their employees about social engineering techniques, regulate their online presence, and implement strong access controls such as two-factor authentication.

2. **Weaponization:** Attaching a remote access trojan to an exploit in a deliverable payload, usually by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents act as the weapon available. Attackers package their exploits into a form that can be used against the target, such as crafting phishing emails or creating malicious payloads. Organizations can avoid these by employing email filters, educate employees on spotting phishing attempts, and use anti-malware tools to detect and block weaponized attacks.

3. **Delivery:** Transfer of the weapon to the targeted environment. The three most common payload delivery vectors armed by APT actors, as observed by the Lockheed Martin Computer Incident Response Team (LM-CIRT) for the years 2004-2010, are email attachments, websites, and USB removable media. The attackers deliver the weaponized exploit to the target, usually through email attachments, or exploit kits. Deployment of network intrusion detection and prevention systems, web application firewalls can be done by organizations to detect and block malicious delivery attempts.

4. **Exploitation:** Once the weapon is delivered to victim host, the exploit triggers intruders' code. In most cases, the exploit targets a vulnerability in an application or operating system, but it could also happen simply exploit the users themselves or take advantage of an operating system feature that runs automatically. Regular patching, vulnerability scans, and penetration testing can help organizations identify and address the vulnerabilities before they are exploited.

5. **Installation:** Installing a remote access trojan or backdoor on the victim's system makes the adversary to maintain persistence in the environment. Attackers establish a foothold within the target's network by installing malware, backdoors, or other persistent methods. To prevent and help detect installation attempts, end-point protection solutions, network segmentation, and intrusion detection systems should be employed.

6. **Command and Control (C2)**: Typically, compromised hosts need to send outgoing beacons to an Internet controller server to establish a C2 channel. APT malware mostly requires manual interaction instead of automatically performing tasks. Once the C2 channel establishes, intruders have \hands on the keyboard" access within the target environment. These attackers establish the communication channels with the compromised system to remotely control it or infiltrate data. To detect and block command and control activities, implementing strong access controls, monitoring

network traffic, and utilizing security information and event management (SIEM) systems should be deployed.

7. **Actions on Objectives** - Only now, after going through the first six stages, intruders can take actions to achieve their original objectives. Alternatively, the intruders may only want to access the initial victim box for use as a springboard to compromise additional systems and move laterally within the network. Robust data loss measures, strong encryption, network segmentation, and incident response plans can help in mitigating the impact of these objectives.

The Unified Kill Chain

The Unified Kill Chain which was developed through a hybrid research approach, combining design science with qualitative research methods. The model was first published in the Executive Master's thesis of Paul Pols entitled "The Unified Kill Chain: modeling Fancy Bear attacks" at the Cyber Security Academy [25]. The Unified Kill Chain extends and combines existing models, such as Lockheed Martins' Cyber Kill Chain® [21] and MITRE's ATT&CK™ for Enterprise

The Unified Kill Chain		
1	Reconnaissance	Researching, identifying and selecting targets using active or passive reconnaissance.
2	Resource Development	Preparatory activities aimed at setting up the infrastructure required for the attack.
3	Delivery	Techniques resulting in the transmission of a weaponized object to the targeted environment.
4	Social Engineering	Techniques aimed at the manipulation of people to perform unsafe actions.
5	Exploitation	Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
6	Persistence	Any access, action or change to a system that gives an attacker persistent presence on the system.
7	Defense Evasion	Techniques an attacker may specifically use for evading detection or avoiding other defenses.
8	Command & Control	Techniques that allow attackers to communicate with controlled systems within a target network.
9	Pivoting	Tunneling traffic through a controlled system to other systems that are not directly accessible.
10	Discovery	Techniques that allow an attacker to gain knowledge about a system and its network environment.
11	Privilege Escalation	The result of techniques that provide an attacker with higher permissions on a system or network.
12	Execution	Techniques that result in execution of attacker-controlled code on a local or remote system.
13	Credential Access	Techniques resulting in the access of, or control over, system, service or domain credentials.
14	Lateral Movement	Techniques that enable an adversary to horizontally access and control other remote systems.
15	Collection	Techniques used to identify and gather data from a target network prior to exfiltration.
16	Exfiltration	Techniques that result or aid in an attacker removing data from a target network.
17	Impact	Techniques aimed at manipulating, interrupting or destroying the target system or data.
18	Objectives	Socio-technical objectives of an attack that are intended to achieve a strategic goal.

Fig. 2: The Unified Kill Chain

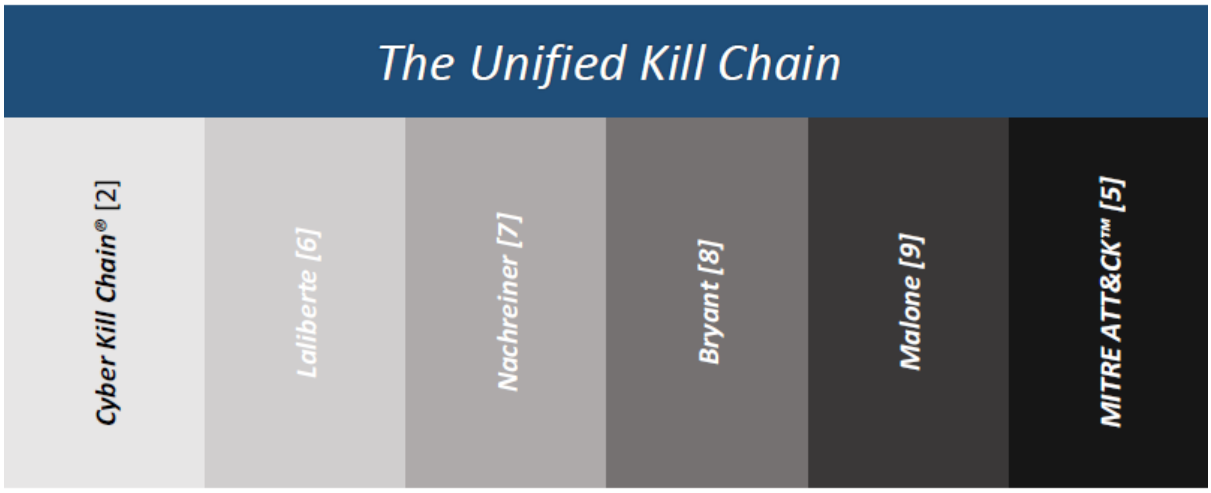

Fig. 3: The Unified Kill Chain II

IV. Discussion

The discussion section focuses on the application of AI in cybersecurity, specifically within the Cyber Kill Chain framework. It highlights the challenges of traditional security architectures and the need for innovative and intelligent security defense methodologies.

The literature review section provides an overview of key components of cybersecurity, including identify, asset management, automated configuration management, automated security control validation, governance, risk assessment, and automated vulnerability identification and assessment.

The theoretical framework introduces the Cyber Kill Chain model and its limitations, leading to the proposal of a Unified Kill Chain model. The Unified Kill Chain addresses the shortcomings of the traditional Cyber Kill Chain by incorporating additional phases and explicitly considering factors such as social engineering, attack objectives, and impact. The benefits of the Unified Kill Chain model in understanding and defending against advanced cyber-attacks are highlighted.

Overall, the discussion section highlights the potential of AI in strengthening cybersecurity defences and addresses the limitations of traditional security approaches.

V. Conclusion

In conclusion, the application of AI in cybersecurity offers promising solutions to address the evolving threat landscape. AI techniques, such as machine learning, anomaly detection, and behavioural analysis, have shown great potential in enhancing various aspects of cybersecurity.

AI has the potential to significantly enhance cybersecurity defences by automating processes, improving threat detection, and enabling proactive defence measures. However, challenges such as data quality, adversarial attacks, and privacy concerns need to be addressed for successful implementation. Further research and development are essential to fully leverage the power of AI in cybersecurity and stay ahead of evolving cyber threats.

References

[1] Wu J, Dong MX, Ota K, et al., 2018. Big data analysis-based secure cluster management for optimized control plane in software-defined networks. *IEEE Trans Netw. Serv. Manag, 15(1):27-38.* https://doi.org/10.1109/TNSM.2018.279900

[2] V.G. Promyslov, K.V. Semenkov, A.S. Shumov, A clustering method of asset cybersecurity classification, *IFAC-PapersOnLine* 52 (13) , (2019), pp. 928–933.

[3] K. Millar, A. Cheng, H.G. Chew, C.C. Lim, Operating system classification: a minimalist approach, *International Conference on Machine Learning and Cybernetics (ICMLC)*, (2020), pp. 143–150.

[4] A. Aksoy, M.H. Gunes, Automated iot device identification using network traffic, *IEEE International Conference on Communications (ICC)*, (2019), pp. 1–7.

[5] A. Sivanathan, H.H. Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath, V. Sivaraman, Classifying IoT devices in smart environments using network traffic characteristics, IEEE Trans. Mobile Comput. 18 (8) (2018) 1745–1759.

[6] I. Cviti´c, D. Perakovi´c, M. Periˇsa, B. Gupta, Ensemble machine learning approach for classification of IoT devices in smart home, *Int. J. Machine Learn. Cybernetics* 12, (11), (2021) 3179–3202.

[16] H. Cam, Online detection and control of malware infected assets, *IEEE Military Communications Conference (MILCOM)*, (2017), pp. 701–706.

[7] H.I. Kure, S. Islam, M. Ghazanfar, A. Raza, M. Pasha, Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system, Neural Comput. App. 34 (1) (2022) 493–514.

[8] M. Vega-Barbas, V.A. Villagr´a, F. Monje, R. Riesco, X. Larriva-Novo, J. Berrocal, Ontology-based system for dynamic risk management in administrative domains, Appl. Sci. 9 (21) (2019) 4547.

[9] B. Tozer, T. Mazzuchi, S. Sarkani, optimizing attack surface and configuration diversity using multi-objective reinforcement learning, *IEEE 14th International Conference on Machine Learning and Applications*, (2015), pp. 144–149.

[10] L.E. García-Hern´andez, A. Tchernykh, V. Miranda-L´opez, M. Babenko, A. Avetisyan, R. Rivera-Rodriguez, G. Radchenko, C.J. Barrios-Hernandez, H. Castro, A.Y. Drozdov, Multi-objective configuration of a secured distributed cloud data storage, *Latin American High Performance Computing Conference*, (2019), pp. 78–93.

[11] M. Sharifi, F. Eugene, J.G. Carbonell, Learning of personalized security settings, *IEEE International Conference on Systems, Man and Cybernetics*, (2010), pp. 3428–3432.

[12] D. Bringhenti, G. Marchetto, R. Sisto, F. Valenza, F.J. Yusupov, Towards a fully automated and optimized network security functions orchestration, *4th International Conference on Computing, Communications and Security (ICCCS)*, (2019), pp. 1–7.

[13] A.J. Varela-Vaca, R.M. Gasca, J.A. Carmona-Fombella, M.T. G´omez-L´opez, AMADEUS: towards the AutoMAteD secUrity teSting, *Proceedings of the 24th ACM Conference on Systems and Software Product Line*, (2020), pp. 1–12.

[14] Y. Liu, A. Sarabi, J. Zhang, P. Naghizadeh, M. Karir, M. Bailey, M. Liu, Cloudy with a chance of breach: forecasting cyber security incidents, *24th USENIX Security Symposium (USENIX Security 15)*, (2015), pp. 1009–1024.

[15] L.V. Stepanov, A.S. Koltsov, A.V. Parinov, Evaluating the cybersecurity of an enterprise based on a genetic algorithm, *International Russian Automation Conference*, 2020, pp. 580–590.

[16] V.L. Narasimhan, Using deep learning for assessing cybersecurity economic risks in virtual power plants, *7th International Conference on Electrical Energy Systems (ICEES), (2021)*, pp. 530–537.

[17] H.H. Nguyen, D.M. Nicol, estimating loss due to cyber-attack in the presence of uncertainty, *IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications* (TrustCom), (2020), pp. 361–369.

[18] C. Ponsard, V. Ramon, M. Touzani, Improving cyber security risk assessment by combined use of i* and Infrastructure Models, *the 14th International iStar Workshop*, (2021), pp. 63–69.

[19] T. Saha, N. Aaraj, N. Ajjarapu, N.K. Jha, SHARKS: smart hacking approaches for RisK scanning in internet-of-things and cyber-physical systems based on machine learning, *IEEE Trans. Emerg*, 10 (2), (2021), pp. 870–885.

[20] J. Straub, Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT&CK and STRIDE Frameworks as Blackboard Architecture Networks, IEEE International Conference on Smart Cloud (SmartCloud), (2020), pp. 148-153.

[21] Q. K. Ali Mirza, M. Brown, O. Halling, L. Shand, & A. Alam, Ransomware Analysis using Cyber Kill Chain, 8th International Conference on Future Internet of Things and Cloud (FiCloud), (2021), pp. 58-65.

[22] P. Toropainen, Utilizing Cyber Security Kill Chain model to improve SIEM capabilities, School of Technology, Degree Programme in Information Technology, Cyber Security, (2020).

[23] A. Villalón-huerta, H. M. Gisbert, & I. Ripoll-ripoll, SOC Critical Path: A Defensive Kill Chain Model, IEEE Access, 10, (2022), pp. 13570-13581.

[24] E. M. Hutchins, M. J. Clopperty, R. M. Amin, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, LM-White-Paper-Intel-Driven-Defense, Lockheed Martin Corporation.

[25] P. Pols, The-Unified-Kill-Chain, Raising Resilience against advanced cyber-attacks, white paper, released under GNU GPL v2, version 1.3, (2023)

26. Kaur R, Gabrijelčič D, Klobučar T. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion. 2023 Apr 7:101804.