International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.020 ISSN: 2581-4621

SURVEY ON CYBER KILL CHAIN

Manasa K
[1]*Assistant professor,*
CSE(CS) Department, CVR College of Engineering, Hyderabad, Telangana, India,
Corresponding author emailed: [1]kmanasa44@gmail.com

Abstract:
A series of models referred to as "kill chain models" describe the numerous steps or measures an attacker would generally follow in order to carry out a successful cyberattack. The models assist cybersecurity experts and companies in comprehending the adversaries' strategies and tactics so they can effectively counter such attacks. Lockheed Martin's "Cyber Kill Chain" is one of the most popular kill chain models. To identify follow-on attacks, traditional attack detection methods employ pre-existing databases containing recognized signatures related to formerly utilized tools and malicious activity observed in earlier cyberattacks. Cyber threat performance and effectiveness can be greatly enhanced by security teams if they adopt the new Cyber Kill Chain model. The model standardizes the stages by providing [1] a uniform and organized pattern. Teams can collaborate effectively because everyone is on the same page when it comes to the steps and goals. Cyber Kill Chain's formal process allows it to easily recognize certain areas of weakness in detection and response functions. Teams can identify specific areas where their defensive systems are lacking or weak by tracking each phase of the kill chain. [2] They can enhance their overall security stance and actively address these vulnerabilities with this information.
Keywords: Kill chain models, Cyber Kill Chain, Cybersecurity, Threat detection

1. INTRODUCTION

In fact, technology has introduced many advantages to people, organizations, and nations, but they are also exposed to several dangers on a daily basis. Adversarial actors, foreign nations, terrorist organizations, and organized crime know these risks all too well and actively use them for nefarious ends, from cybercrime to cyber warfare.[2] Here, Computer Network Operations (CNO) feature prominently in offensive and defensive cyber operations. CNO involves a set of capabilities utilized to launch cyber-attacks against an adversary's computer networks, to defend one's own networks, and to exploit enemy computers for intelligence gathering. Offensively, CNO permits specific attacks and exploitations for the purpose of disrupting or undermining the enemy's key infrastructure, stealing sensitive data, or gaining a strategic digital advantage.

Defensively, CNO is imperative to protecting an organization or nation's digital data and information.

It involves the implementation of different types of cybersecurity to identify, prevent, and reduce cyber threats and attacks. This includes activities such as vulnerability scanning, intrusion detection, incident response, and threat intelligence analysis. In the current cyber environment, the distinction between offensive and defensive CNO may be blurred.[2] Defensive operations involve leveraging offensive techniques for reconnaissance and gathering intelligence on potential threats. On the other hand, offensive operations can include preemptive strikes to disorient or incapacitate potential aggressors before they are able to attack.

The interdependence of cyberspace and the dependence on digital technologies make CNO an essential element of national security and global affairs. States and organizations spend a lot of resources building their CNO capabilities in order to remain competitive in cyberspace and defend their interests.

The nature of CNO, however, also poses ethical and legal concerns. The use of offensive cyber capability must be controlled appropriately so that it would not have unforeseen consequences and comply with international law and norms. Collateral damage potential, conflict escalation, and

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.020 ISSN: 2581-4621

unintended harm to innocent civilians are reasons why responsibility and accountability are crucial in employing CNO.

2. METHODOLOGY

In the first phase in the Cyber Kill Chain, that of reconnaissance, attackers acquire important data about the organization or system that they are attempting to breach. Reconnaissance consists of both passive and active methods for recognizing potential vulnerabilities, weaknesses, and valuable assets. Public information from websites, social media, or public records is required for passive reconnaissance. Active reconnaissance involves actions such as network probing, port scanning, and data collection by talking to the target directly. [2].

Cyber Kill Chain.It is important for organizations to utilize strong cybersecurity practices, such as regular patching and updating of software, to reduce the likelihood of successful weaponization and minimize the attack surface that can be used by potential attackers. Active threat hunting and ongoing monitoring are also important to identify any signs of weaponization activity early and prevent potential threats from growing before they become serious.

Installation is the fifth phase of the Cyber Kill Chain, in which the attackers gain a persistent foothold on the infected system or network. After the initial exploitation is effective, attackers move on to deploy a range of tools, malware, or backdoors that make it possible for them to persist and control the system.

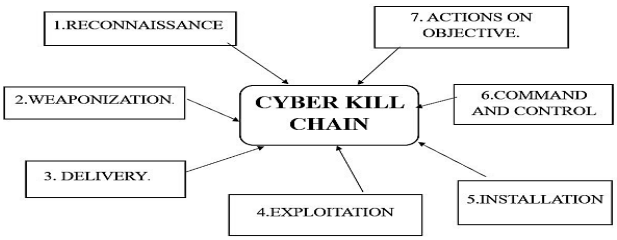
Extra payloads and modules that assist the attacker in bypassing security controls, persist even after the machine has been restarted, and avoid detection by security products are distributed during installation. Before you use Nmap or another Kali Linux reconnaissance tool, ensure you have the necessary permissions. Recon-ng is a highly featured reconnaissance framework that assists in the collection of information from numerous APIs and web-based sources. The Harvester is an email address, subdomains, and other publicly available information from social media and search engines that is a target. Shodan is search engines that allow the user to search for specific types of internet-connected devices, including cameras, servers, routers, and more. An anonymous intelligence (OSINT) tool, Maltego, assists in link analysis and data mining. Case Study: Ransomware attack on a factory by means of social media, job postings, and publicly available tools, the attackers performed extensive reconnaissance of the manufacturing firm, discovering information about its staff, network structure, and possible entry points. The employment of weapons the attackers crafted a spear-phishing email aimed at the finance department based on the information they had gathered through reconnaissance.

The email looked like it came from the CEO of the company, asking the recipient to look at a so-called contract proposal attached to the email in a hurry.

Cyber Kill Chain

CKC is among the most popular frameworks used to detect, prevent, and identify advanced persistent cyber threats.

In the phases of CKC, few researchers have suggested techniques for early detection of cyber threats. The cyber death chain targets APTs and malware-driven attacks [10]. The idea of CKC has been advanced and extended to be used against internal threats and industrial control systems (ICS), i.e., the extended cyber kill chain and the ICS cyber kill chain, respectively. Both of these chains of death can be applied together on railways.



International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.020 ISSN: 2581-4621

Figure 1:Cyber kill chain

External Cyber Kill Chain

An initial CKC model was developed by Lockheed Martin to attack the corporate network. The seven stages of this model are Reconnaissance is the initial phase of the model, arguably one of the hardest phases to identify from a security monitoring viewpoint, is the planning phase of the cyber-attack. The attacker looks for and procures information regarding the organization background, assets, and individual employees using social sites, conferences, blogs, mailing lists and other network tracing tools. The gathered data is utilized in later stages in order to deliver payload (the actual message intended to cause malicious activity) to the target system.Weaponize: The operation preparation stage is the second stage of the model. It consists of the integration of a remote access Trojan (RAT) with an exploit to a deliverable payload, which is usually achieved through an automated tool (weaponizer) [15].

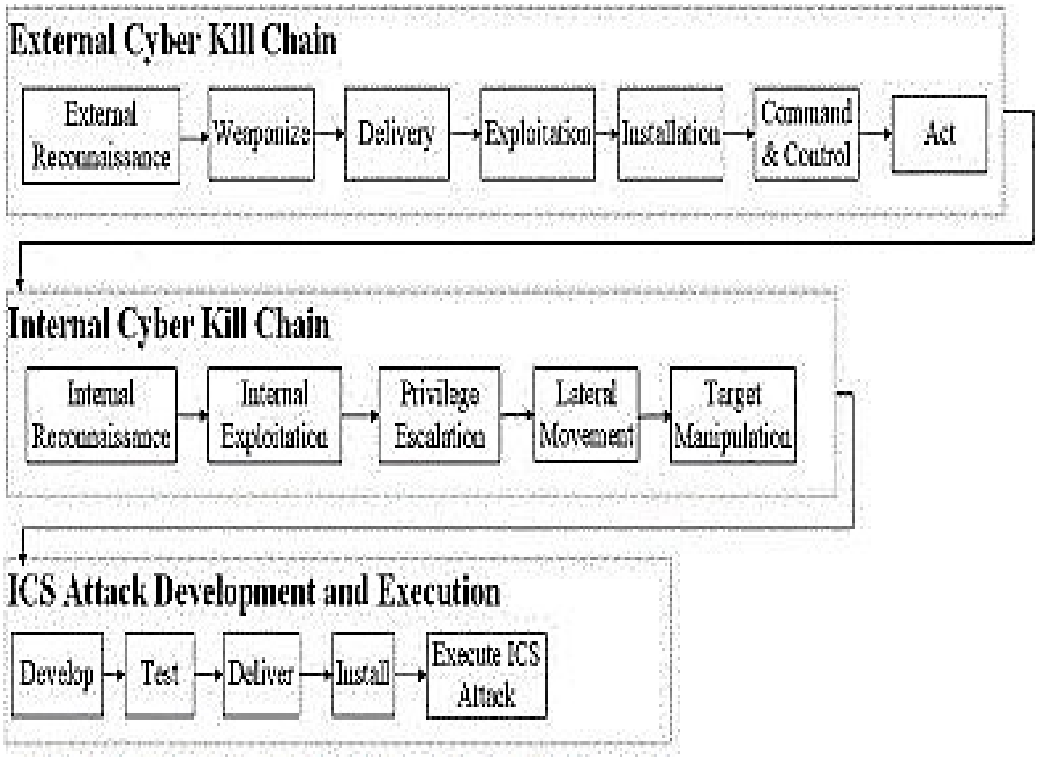


Figure 2 :Unified extended cyber kill chain and ICS cyber kill chain .

3. A CASE OF RAILWAY SCADA EXAMPLE

Consider a multi-phase cyberattack on a railway SCADA system, where a threat agent compromises the system and causes it to transmit a malicious or unregistered order. Several strategies from the RDKC matrices can be chosen to reduce the risk for this attack in advance, as shown in Figure 3[11]. For example, defenders can use detection technologies like NIDS or web analytics to guard against the initial phase, or external reconnaissance. By providing certain fake weaponized codes or fake registration, the defense can deceive the attacker throughout the second phase (weaponized). Figure 3 shows how the defender can use deep packet inspection to identify the attacker within the third phase (delivery).

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.020 ISSN: 2581-4621

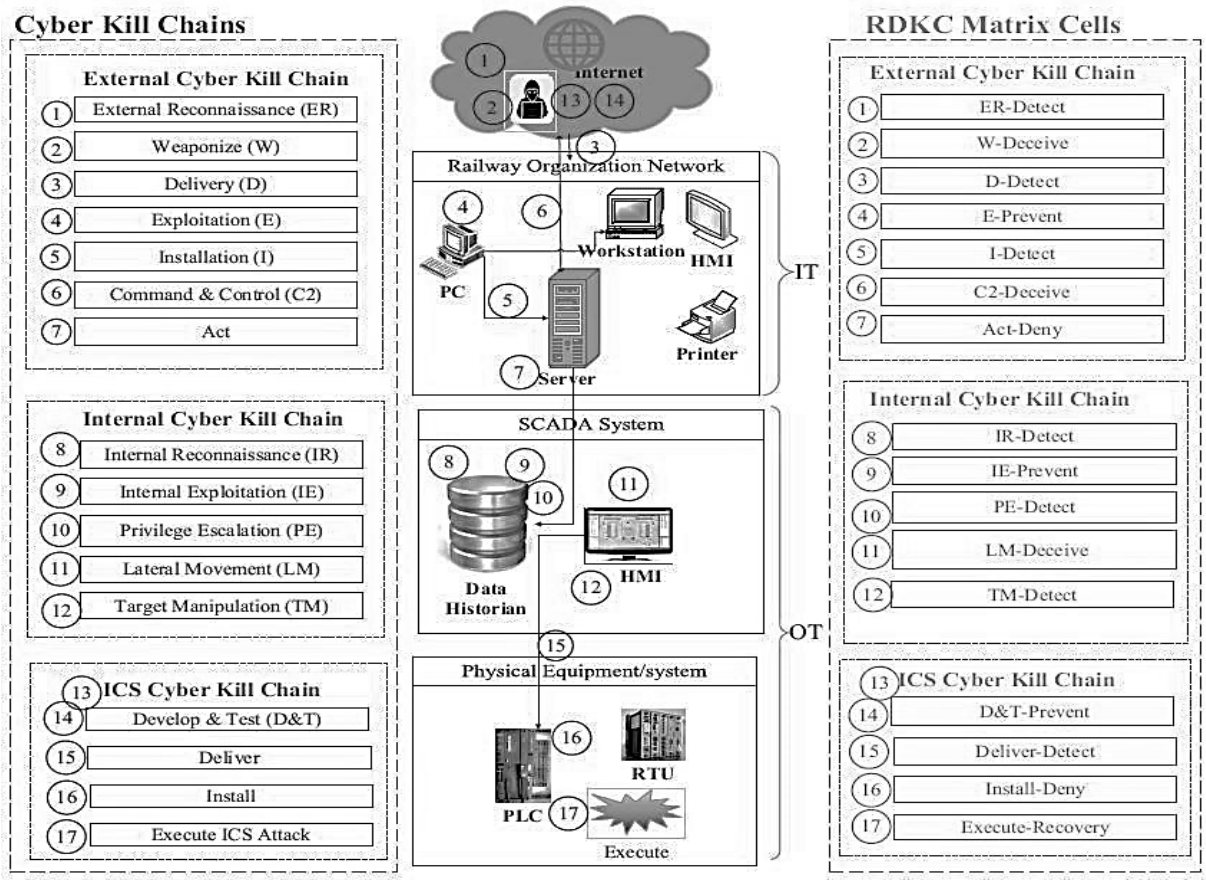


Figure 3: An example of a railway SCADA system that uses a computerized kill chain and a railway defense kill chain to lower the danger of cyberattacks.

4. The Pentration Probabilities for Each Cyber Kill Chain Phase

This work began emulating the probability of a cyberattack's penetration with varying security controls established in each step down the cyber kill chain for it to explore the given framework. The considered and showcased technologies within the RDKC matrix [12] are these security controls. In order to protect against the cyberattack, the defender may opt to implement some security controls at every step along the cyber kill chain. is one of the theoretical outcomes of the penetration probabilities based on how likely a cyberattack at every stage of the cyberkill chain is. The probability of defense in this scenario varies from 11% to 20% for the initial two steps and from 21% to 30% for the last five steps (figure 4).

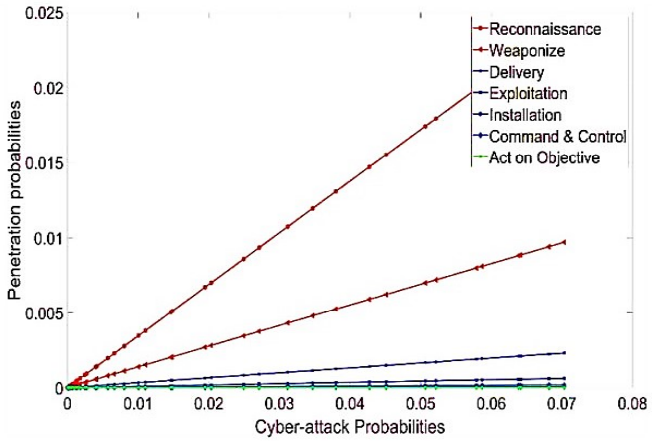


Figure 4: Probabilities of cyberattack penetration at every phase of the cyberkill chain.

DOI:10.46647/ijetms.2025.v09si01.020 ISSN: 2581-4621

4. CONCLUSION

In short, Cyber Kill Chain is a valuable model for understanding and analyzing the progression of cyber attacks. It provides a systematic approach to threats identification and mitigation in a structured process. Through compartmentalizing the attack life cycle into distinct phases, organizations can develop targeted defense tactics, enhance incident response, and enhance overall cybersecurity stance.

The future of Cyber Kill Chain lies in its adaptation and evolution to deal with the ever-changing cyber threat landscape. As technology continues to evolve, the model must include AI, ML, and behavioral analysis to detect sophisticated threats and anticipate attacker actions. In addition, dealing with such emerging challenges as cloud security, IoT, and quantum computing will be required. In addition, promoting the exchange of threat intelligence, being human-centric, and proactive defense will be critical elements in staying ahead of cyber threats. Automation, orchestration, and deception techniques need to be utilized to successfully counter threats and mislead attackers. Finally, the Cyber Kill Chain should facilitate cooperation among organizations, promote ongoing improvement, and conform to zero-trust principles. With its capacity to stay dynamic and contextually aware, the Cyber Kill Chain will allow organizations to successfully detect, reduce, and prevent cyber threats, safeguarding key data, infrastructure, and user privacy.

5. REFERENCES

[1] Athanasiosdimitriadis, efstratioslontzetidis3, boonsermkulvatunyou, nenadivezic2, dimitris gritzalis 4, and ioannis mavridis is the “fronesis: digital forensics-based early detectionof ongoing cyber-attacks”.

[2] Soc critical path: a defensive kill chain model antonio villalón-huerta 1, hector marco gisbert 2, (senior member, ieee), and ismael ripoll-ripoll 2.

[3] M. P. Barrett, ‘‘Framework for improving critical infrastructure cybersecurity, version

[4] 1.1,’’ NIST Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. CSWP 04162018, Apr. 2018.

[5] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, vol. 1. New York, NY, USA: Academic, 2011.

[6] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, ‘‘Intrusion detection system: A comprehensive review,’’ J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16–24, 2013.

[7] MANDIANT. M-Trends 2021: Insights into Today’s Top Cyber Trends and Attacks. Accessed: Sep. 5, 2021. [Online]. Available: https://www.fireeye.com/current- threats/annual-threat-report/mtrends.html.

[8] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, ‘‘MITRE ATT&CK: Design and philosophy,’’ The Mitre Corporation, McLean, VA, USA, Tech. Rep. 10AOH08A-JC, Mar. 2020. [6] EU

[9] ATT&CK Community. Directory of ATT&CK Open-Source Tools. Accessed: Mar. 8, 2022. [Online].Available:https://www.attackcommunity.org/directory/.

[10] ‘‘Information operations primer. fundamentals of information operations,’’Dept. Mil. Strategy,U.S. Army War College, Planning, Oper., Carlisle, PA,USA, Tech. Rep., Nov. 2011.

[11] F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé,and G.-J. Ahn, ‘‘Matched and mismatched SOCs: A qualitative study on security operations center issues,’’ in Proc. ACM SIGSAC Conf. Comput.Commun. Secur., Nov. 2019, pp. 1955–1970.

[12] C. Zimmerman, Cybersecurity Operations Center. McLean, VA, USA: TheMITRE Corporation, 2014.

[13] J. M. Brown, S. Greenspan, and R. Biddle, ‘‘Incident response teams in IToperations centers: The T-TOCs model of team functionality,’’ Cognition,Technol. Work, vol. 18, no. 4, pp. 695–716, Nov. 2016.

[14] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, ‘‘Security operationscenter: A systematic

DOI:10.46647/ijetms.2025.v09si01.020 ISSN: 2581-4621

study and open challenges,'' IEEE Access, vol. 8, pp. 227756–227779, 2020.
[15] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, vol. 5, no. 4, pp. 1-10, 2011.
[16] M. K. Rogers and K. Seigfried, "The Future of Computer Forensics: A Needs Analysis Survey," Computers & Security, vol. 23, no. 1, pp. 12-16, 2004.