Major Ways in Which Machine Learning Improve Cyber-Attack Predictability in The Department of Defense Supply Chain

Jeggo Paolo V. DyCok

Jdyco001@odu.edu

Old Dominion University

IDS 300W: Interdisciplinary Studies

Dr. Kathryn LaFever

April 8, 2023

ABSTRACT

Cybersecurity is a crucial issue in the Department of Defense (DoD) supply chain, with the system highly vulnerable to cyber-attacks that could have significant consequences. Machine learning has emerged as a promising solution to enhance cyber-attack predictability, a critical aspect of ensuring the DoD supply chain's security and resilience. This research explores the question of how machine learning can be leveraged to enhance cyber-attack predictability in the DoD supply chain. The interdisciplinary approach to researching and writing this paper allows for the integration of insights from computer science, cybersecurity, and logistics management to address the multifaceted challenge. The paper is particularly pertinent to students pursuing a degree in cybersecurity or logistics management, and those interested in interdisciplinary research on complex systems. The study aims to contribute to the development of more effective cybersecurity strategies for the DoD supply chain by examining how machine learning can improve cyber-attack predictability. Through a comprehensive review of relevant literature, data analysis, and case studies, the research will investigate the feasibility, effectiveness, and limitations of machine learning in enhancing cybersecurity in the DoD supply chain. The study's findings are expected to provide practical insights and recommendations for policymakers, cybersecurity professionals, and researchers working in this area. By leveraging machine learning to enhance cyber-attack predictability, the DoD supply chain's security and resilience can be significantly strengthened, ensuring the protection of the nation's critical assets.

Key words: Cyber Physical Systems, Machine Learning, Deep Learning, Internet of Things

How Does Machine Learning Improve Cyber-Attack Predictability in The Department of Defense Supply Chain?

INTRODUCTION

The modern world is becoming increasingly digitized, with technology integrated into every facet of our lives. While this has brought with it numerous benefits, it has also exposed us to new and ever-evolving threats. This becomes more evident in the Department of Defense (DoD) supply chain, where the increasing use of technology poses a significant cybersecurity challenge. As a cybersecurity major, I am very interested in exploring how machine learning can be used to augment the predictability of cyber-attacks in this context. I believe that this research has the potential to yield critical insights into the interplay between machine learning, cybersecurity, and supply chain management. By defining and exploring these key terms, this research aims to lay the groundwork for a more comprehensive understanding of how machine learning can be used to address cybersecurity risks in the supply chain management and its potential benefits and conflicts. Through an interdisciplinary approach that draws upon the unique perspectives and methodologies of each field of study, I hope to analyze the problem holistically and contribute to the ongoing conversation about how to effectively secure the DoD supply chain against cyber-attacks. This research is more important than ever given the increasing reliance on technology in the DoD supply chain and the potential implications of a cybersecurity breach.

MACHINE LEARNING

Machine learning refers to the study and implementation of artificial intelligence that enables machines to learn from data and improve their performance without being explicitly programmed. The term was coined by Arthur Samuel in the 1950s, when he used the technique to teach a computer how to play checkers. Since then, advances in computing power and data storage have enabled the development of innovative machine learning-based products like Google and Netflix's recommendation engine and self-driving cars. Today, machine learning is a vital component of data science, where statistical methods and algorithms are used to classify, predict, and uncover insights from large datasets. As big data continues to grow, the demand for skilled data scientists will continue to rise. Machine learning algorithms are primarily created using frameworks like TensorFlow and PyTorch due to their robustness of machine learning functions, which accelerates solution development and enables businesses to make data-driven decisions.

In the field of cybersecurity, machine learning has been widely adopted to identify patterns in cyber-attacks and predict future attacks, providing real-time processing, sensing, and activation across innovative systems. The internet has changed how people learn and work but has also brought security threats. Cybersecurity is a set of technologies and procedures created to protect computers, networks, programs, and data from unauthorized access, alteration, or destruction. According to Yang et al. (2018), "ML is a branch of AI and is closely related to (and often overlaps with) computational statistics, which also focuses on prediction making using computers." Additionally, they state that "DL is a new field in machine-learning research. Its motivation lies in the establishment of a neural network that simulates the human brain for analytical learning. It mimics the human brain mechanism to interpret data such as images, sounds and texts." It is worth noting that machine learning (ML) and deep learning (DL) methods are used for cybersecurity applications, especially in network intrusion detection (IDS). According to Yang et al. (2018), there are three main types of network analysis for IDSs: misuse-based, also known as signature-based, anomaly-based, and hybrid.

According to Radaniliev et al. (2021), machine learning as it relates to cybersecurity aims to show how AI implementation can be utilized to predict or simply mitigate the scale of cyber-attacks, "by automating aspects such as intelligence gathering, target selection, and attack execution." Ghillani (2022) highlights that incorporating machine learning systems can lead to breakthroughs in artificial intelligence for cybersecurity. An interdisciplinary approach that combines computer science, cybersecurity, and logistics management can provide diverse insights to address the complex issue of supply chain cybersecurity. By utilizing the power of machine learning, computer scientists can devise effective strategies to improve the security and resilience of the DoD supply chain.

CYBERSECURITY

Cybersecurity, according to the National Institute of Standards and Technology (NIST), aims to secure information systems from theft or damage to the hardware, software, and data, as well as from disruption or misdirection of services they provide. In line with this, Cyber-Physical Systems, or CPS, require anti-counterfeiting and supply chain risk management to address malicious components in the supply chain that have been modified from their intended design to cause disruption or perform illegal functions (Ghillani, 2022). Given that the DoD supply chain involves interconnected devices and systems, it is highly vulnerable to cyber-attacks, making cybersecurity a crucial discipline that plays a vital role in understanding how machine learning can improve the predictability of such attacks.

To ensure the security and resilience of the DoD supply chain, cybersecurity professionals utilize techniques, systems, tools, and workflows that empower acquisition departments for supply chain data analytics for cybersecurity compliance and information assurance (Maule, 2021). The practice of cybersecurity aims to prevent damage to, protect, and restore computer systems, electronic communications, and information contained therein to ensure availability, integrity, authentication, confidentiality, and nonrepudiation. Machine learning techniques, when integrated with cybersecurity with its data analytics capabilities, can identify patterns in cyber-attacks, mitigate risks, and enhance the predictability of these attacks. By understanding the role of cybersecurity in machine learning, comprehensive insights can be gained to improve the security and resilience of the DoD supply chain. Therefore, the application of machine learning techniques to cybersecurity is crucial in enhancing the predictability of cyber-attacks in the DoD supply chain.

SUPPLY CHAIN MANAGEMENT

The Department of Defense (DoD) supply chain is a critical system that requires robust cybersecurity measures to ensure its security and resilience. The supply chain encompasses various processes and factors involved in the acquisition, production, and distribution of goods and services. According to the annual industrial capabilities report by the Pentagon’s Office of Manufacturing and Industrial Base Policy, the industrial base of the weaponry sector is particularly strained, due to the irregular flow of procurement and the lack of new designs being internally developed. As a result, measuring and managing information on key operational and performance parameters is critical. However, the complexity of this system presents a challenge to the acquisition role, which lacks the resources and technical expertise to accomplish comprehensive and continuous cybersecurity assessment across the supply chain and life cycle of an asset (Maule, 2021). To enhance the predictability of cyber-attacks in the DoD supply chain, interdisciplinary research that combines supply chain management with computer science and cybersecurity is necessary.

The potential of machine learning to improve cybersecurity can be further enhanced through the integration of Internet of Things theories and Cyber-Physical Systems (Radaniliev et al., 2021). In addition to this, Cantelmi et al. (2020) proposed a framework for managing technical incidents from an organizational perspective, which can be used alongside other strategies like reverse logistics. This framework, called Learning from Incident (LFI), consists of several components: identification and response, reporting, investigation, making recommendations, and communication. LFI emphasizes the importance of establishing an appropriate identification threshold to detect deviations from normal behavior, proper reporting to investigate incidents, identifying the causal structure of incidents, and disseminating the findings and recommendations to enhance organizational learning. By leveraging these multiple disciplines and frameworks, more effective cybersecurity strategies can be developed for the DoD supply chain.

COMMON GROUND

Machine learning, cybersecurity, and supply chain management are all interconnected fields that play important roles in the development and implementation of modern technology. One key area where these fields intersect is in the detection and prevention of malicious attacks on electronic devices. As Amir et al. (2021) note, machine vision and artificial intelligence can be used to monitor electronic components such as printed circuit boards (PCBs) and detect any malicious chips hidden within them. This demonstrates the importance of utilizing advanced technologies to ensure the security and safety of electronic devices, which is essential for protecting sensitive information and preventing potentially catastrophic cyber-attacks.

Another area where machine learning, cybersecurity, and supply chain management intersect is in the assessment and management of key operational and performance parameters. As Cantelmi et al. (2020) point out, measuring and managing this information is critical for ensuring the smooth functioning of the industrial base and minimizing the risk of disruptions to the supply chain. By utilizing machine learning and other advanced technologies, companies can more effectively monitor and manage these parameters, enabling them to make better decisions and optimize their operations. This highlights the importance of leveraging advanced technologies to improve the efficiency and reliability of supply chain management.

Finally, the integration of the Internet of Things (IoT), Cyber Physical Systems (CPS), and other advanced technologies is critical for enabling smart manufacturing and meeting customer demands. As Radaniliev et al. (2021) note, this requires a deep understanding of how these technologies interact and can be leveraged to optimize manufacturing processes. By utilizing machine learning and other advanced technologies, companies can better integrate these various components and build more effective smart manufacturing systems. This highlights the importance of cross-disciplinary collaboration and knowledge-sharing between experts in machine learning, cybersecurity, and supply chain management.

DISCIPLINARY CONFLICTS

Machine Learning (ML) has the potential to revolutionize supply chain management by enabling comprehensive analysis of data from multiple technical specializations. However, integrating ML technology in supply chains also presents risks, particularly in the area of cybersecurity. Radaniliev et al. (2021) note that integrating less secure systems in the supply chain can lead to cybersecurity threats. The increase in the number of IoT devices built into digital supply chains can also result in data leaks and significant privacy risks. These potential risks highlight the need for effective cybersecurity measures to protect supply chains from cyber threats.

The integration of third-party service providers in supply chains also poses potential threats to organizations. Yeboah-Ofori et al. (2021) highlight the potential risk of outsourcing business and data to third-party service providers. In such situations, organizations may lose control over their data, thereby exposing it to external threats. Organizations need to ensure that third-party service providers have adequate cybersecurity measures in place to protect their data from cyber threats.

Despite the potential risks associated with the integration of ML in supply chain management, the technology can still be harnessed to improve supply chain management. Maule (2021) notes that ML technology can model the necessary expertise from multiple technical specializations required for comprehensive supply chain analysis. Hyper-connectivity in the digital supply chain must also be promoted in addition to design and process standardization, according to Ghillani (2022). By ensuring the effective integration of ML technology, adequate cybersecurity measures, and hyper-connectivity in the digital supply chain, organizations can achieve comprehensive supply chain analysis while minimizing potential cyber threats.

In conclusion, the integration of ML technology in supply chain management presents both opportunities and challenges. While ML technology can model expertise from multiple technical specializations and improve supply chain analysis, it can also lead to cybersecurity threats if not integrated properly. Organizations need to ensure that third-party service providers have adequate cybersecurity measures in place, and hyper-connectivity in the digital supply chain is promoted alongside design and process standardization. By implementing these measures, organizations can achieve comprehensive supply chain analysis while minimizing potential cybersecurity threats.

CONCLUSION

The Department of Defense (DoD) supply chain is a complex, but essential system that requires extensive cybersecurity measures to ensure its security and resilience due to its importance in national defense. With the increasing sophistication of cyber-attacks, the use of machine learning techniques in computer science and cybersecurity has become crucial in enhancing the predictability of these attacks in the DoD supply chain. However, the effectiveness of machine learning techniques also depends on an interdisciplinary approach that involves supply chain management. To further enhance the predictability of cyber-attacks in the DoD supply chain, the integration of Internet of Things (IoT) theories and Cyber-Physical Systems (CPS) can provide valuable insights. Nonetheless, a potential disciplinary conflict within machine learning, cybersecurity, and supply chain management can arise due to resource allocation and technical expertise. This conflict can lead to a trade-off between cost and efficiency over security measures. Therefore, a multidisciplinary approach that brings together supply chain management, cybersecurity, and machine learning expertise is necessary to address this conflict and develop effective cybersecurity strategies that balance cost, efficiency, and security. Ultimately, the aim of this research is to contribute to the development of more effective cybersecurity strategies for the DoD supply chain.

REFERENCES

Cantelmi, R., Di Gravio, G., & Patriarca, R. (2020). Learning from incidents: A Supply Chain Management Perspective in military environments. *Sustainability*, *12*(14), 5750. https://doi.org/10.3390/su12145750

Cybersecurity - glossary: CSRC. CSRC Content Editor. (n.d.). Retrieved April 5, 2023, from https://csrc.nist.gov/glossary/term/cybersecurity

Ghillani, D. (2022). Deep learning and artificial intelligence framework to improve the cyber security. https://doi.org/10.22541/au.166379475.54266021/v1

Kulkarni, A., & Xu, C. (2021). A deep learning approach in optical inspection to detect hidden hardware trojans and secure cybersecurity in Electronics Manufacturing Supply Chains. *Frontiers in Mechanical Engineering*, *7*. https://doi.org/10.3389/fmech.2021.709924

Maule, R. (2021). *Acquisition Data Analytics for Supply Chain Cybersecurity*. https://doi.org/https://dair.nps.edu/handle/123456789/4320

Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., Maddox, L. T., & Burnap, P. (2020). Cyber risk at the edge: Current and future trends on Cyber Risk Analytics and artificial intelligence in the industrial internet of things and Industry 4.0 Supply Chains. *Cybersecurity*, *3*(1). https://doi.org/10.1186/s42400-020-00052-8

What is machine learning? IBM. (n.d.). Retrieved April 5, 2023, from https://www.ibm.com/topics/machine-learning

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, *6*, 35365–35381. https://doi.org/10.1109/access.2018.2836950

Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber threat predictive analytics for improving Cyber Supply Chain Security. *IEEE Access*, *9*, 94318–94337. https://doi.org/10.1109/access.2021.3087109