The Transformative Integration of Artificial Intelligence with CMMC and NIST 800-171 For Advanced Risk Management and Compliance

Mia Lunati
William & Mary

The Transformative Integration of Artificial Intelligence with CMMC and NIST 800-171 For Advanced Risk Management and Compliance

Mia Lunati

Coastal Virginia Commonwealth Cyber Initiative

Cybersecurity Undergraduate Research Program

Dr. Saltuk Karahan

1 December 2023

Abstract

This paper explores the transformative potential of integrating Artificial Intelligence (AI) with established cybersecurity frameworks such as the Cybersecurity Maturity Model Certification (CMMC) and the National Institute of Standards and Technology (NIST) Special Publication 800-171. The thesis argues that the relationship between AI and these frameworks has the capacity to transform risk management in cybersecurity, where it could serve as a critical element in threat mitigation. In addition to addressing AI's capabilities, this paper acknowledges the risks and limitations of these systems, highlighting the need for extensive research and monitoring when relying on AI. One must understand boundaries when integrating AI into frameworks that ensure the security of sensitive data, otherwise, the ethicality of AI systems is compromised. This paper overviews compliance audits and their intricate relationship with cybersecurity frameworks CMMC and NIST 800-171, underscoring their complementary nature and shared objectives. Finally, the significance of AI in ensuring compliance with these frameworks will be explored, and the transformative potential of AI in automating processes and its advancements in risk management will be discussed.

Introduction

With modern technological advancements, the integration of Artificial Intelligence (AI) serves as a vital step in transforming the future of cybersecurity. Every business and organization must identify and mitigate online threats, and thus the imperative to innovate risk management and compliance has become more pronounced than ever. As such, known cybersecurity models such as the Cybersecurity Maturity Model Certification (CMMC) and the National Institute of Standards and Technology (NIST) Special Publication 800-171 would benefit from the incorporation of AI technology. The use of AI has the potential to revolutionize risk management

and improve adherence to these frameworks, ultimately building resilience against the continuous development of new cyber threats. Utilizing the analytical and predictive capabilities of AI, in addition to its automation potential, organizations would be able to efficiently detect and mitigate risks while also streamlining their compliance efforts. The synergy between AI and established frameworks such as CMMC and NIST 800-171 introduces a possible paradigm shift in cybersecurity operations, wherein AI emerges as an essential component in risk mitigation and navigating compliance mandates.

Purpose and Structure of CMMC and NIST 800-171

NIST 800-171, titled "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," outlines the standards for protecting Controlled Unclassified Information (CUI) when handled by contractors, suppliers, or other non-federal establishments. The importance of protecting CUI from non-federal entities is its essentiality to the functionality of standard government missions and procedures. Examples of CUI include financial data, personally identifiable information (PII), intellectual property, or proprietary business information. And, with the increased reliance on external sources to carry out various functions, NIST 800-171 must ensure and enhance the security of organizations and the protection of CUI. In the official NIST Special Publication 800-171, the three main chapters outline the purpose, fundamentals, and security requirements that any relevant organization must implement. Chapter two discusses the assumptions and process that was put into practice during the development of security requirements while chapter three includes 14 families of requirements that address specific aspects of information security.

TABLE 1: SECURITY REQUIREMENT FAMILIES

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

Figure 1. Security requirement family graph from official NIST 800-171 publication

Overall, the significance of complying with the requirements outlined in NIST 800-171 is its mitigation of cybersecurity attacks and aids the general protection of sensitive information.

On the other hand, the Cybersecurity Maturity Model Certification (CMMC) was developed by the Department of Defense (DoD) to further outline and enhance the cybersecurity practices of contractors and other external suppliers working with the government. Again, CMMC utilizes and builds upon preexisting security practices such as NIST 800-171 to ensure the safety of CUI and Federal Contract Information (FCI) from cyber-attacks. Using a tiered model, CMMC measures an establishment's cybersecurity level by assessing its contract

requirements in relation to its appropriate level of certification.

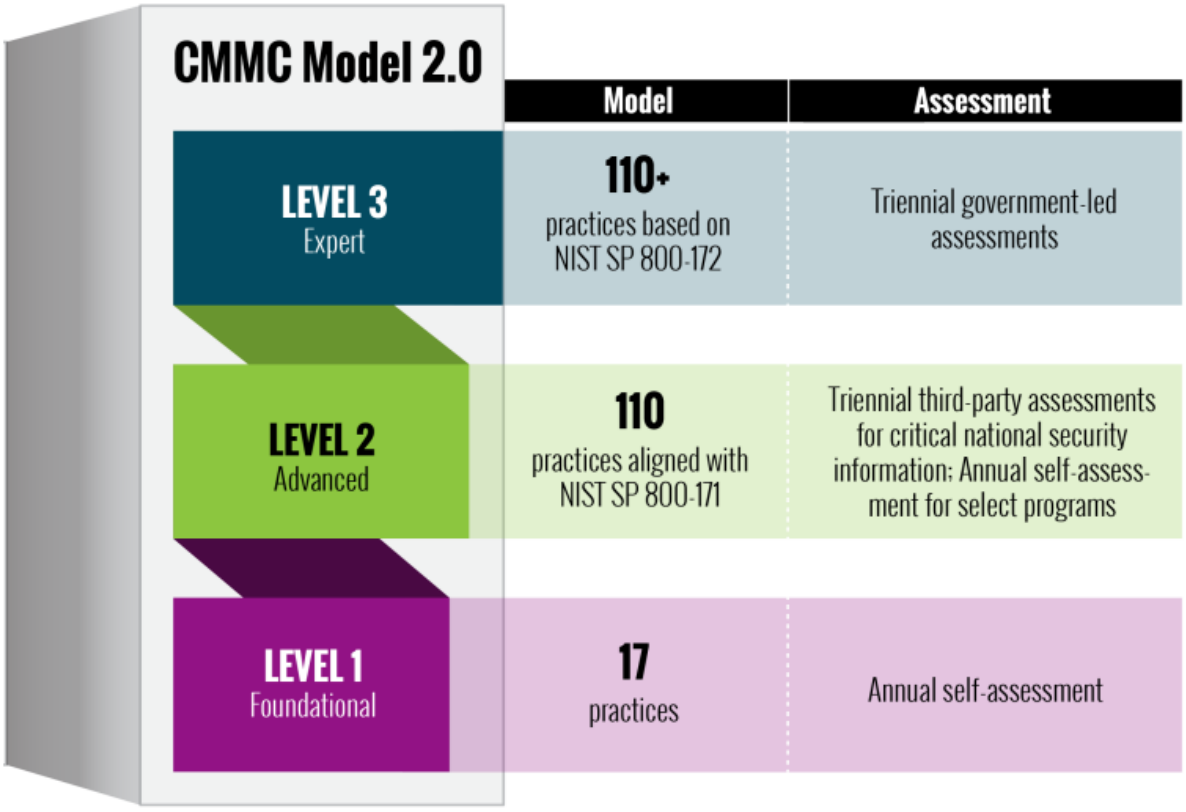

Figure 2. CMMC Model 2.0 from official CMMC Model Overview

The official *CMMC - Model Overview* lists the requirements for each tier as follows:

> "Level 1 focuses on the protection of FCI and consists of only practices that correspond to the basic safeguarding requirements specified in 48 CFR 52.204-21, commonly referred to as the FAR Clause. Level 2 focuses on the protection of CUI and encompasses the 110 security requirements specified in NIST SP 800-171 Rev 2. Level 3 will be based on a subset of NIST SP 800-172 requirements." Pg. 4-5

Organizations handling sensitive government information must prepare and prevent cyber threats, especially prime targets such as the defense industrial base (DIB). The introduction of CMMC was in response to the lack of cybersecurity measures toward DIB contractors and external

personnel and the development of this framework allowed for security practices to be properly enforced and measured, promoting more consistent cybersecurity.

NIST 800-171 and the CMMC both involve enforcing security measures regarding CUI through standardizing cybersecurity frameworks and, while each model provides its comprehensive outline for security practices, CMMC builds upon the elements introduced in NIST 800-171 to create a more elaborate standard for protecting sensitive information. The primary difference between NIST 800-171 and CMMC is that the former outlines 14 main security requirements to protect CUI but does not include specific certification levels like the latter. For one, CMMC utilizes 5 levels of certification to measure an organization's degree of cybersecurity, with each level building upon the former's amount of complexity. However, CMMC does incorporate practices from NIST 800-171, and it uses all 110 of its security controls. Meaning, to obtain a CMMC Level 3 certification, an organization must already comply with NIST 800-171. NIST 800-171 serves as a baseline for CMMC certifications and allows for CMMC to introduce additional security measures such as a tiered model to assess cybersecurity maturity. They are similar frameworks that are frequently referenced in government contracts, especially those handling sensitive information. Compliance with these frameworks is often a prerequisite for securing government contracts and maintaining a robust cybersecurity environment. In this case, CMMC was originally designed to reinforce the security of organizations involved in DoD contracts while, on the other hand, NIST 800-171 is specific to the handling of CUI in non-federal systems. Both frameworks introduce a competitive advantage where CMMC certification enhances the advantage of organizations bidding for DoD contracts and NIST 800-171 regulation paints organizations as reliable and secure partners for government

contracts. They reflect a commitment to cybersecurity and protecting information, building trust and partnerships among government, and sometimes external, sources.

Implementation of CMMC and NIST 800-171

In the case of non-adherence, organizations face various consequences that can critically negatively impact their operations and security. For one, organizations involved in DoD contracts can lose current and potential contracts if they fail to comply with CMMC, especially with the DoD's increasing requirement of achieving specific CMMC certification levels. Similarly, non-adherence with NIST 800-171 will also lead to the loss of government contracts, in the case an organization is dealing with agencies that mandate its requirements. Financial penalties or even lawsuits may occur as well, and government or regulatory agencies may impose a fine for failing to meet cybersecurity standards, especially when dealing with sensitive data. Additionally, organizations may also be excluded from bidding opportunities, limiting their participation in government procurement processes. This is because agencies often will prioritize contractors that have reached a certain level of cybersecurity maturity to ensure the safety and privacy of their information. Relating, the inadequate protection of data that comes with the non-adherence to cybersecurity standards may lead to data breaches and cyberattacks. This could lead to operational disruptions and loss of consumer trust, and companies would have to reallocate resources and invest in new technologies and policies. In short, the proper implementation of cybersecurity framework requirements is necessary to avoid the multifaceted consequences of non-compliance. In doing so, organizations avoid negative impacts on their financial stability, operational continuity, reputation, contractual opportunities, and legal standing. The implementation of frameworks such as CMMC and NIST 800-171 is essential for engaging with government contracts and upholding relationships with clients and stakeholders.

Use of AI in Risk Management

With the evolving complexity of cyber threats, the need for a shift in traditional risk management strategies becomes increasingly apparent. This is because conventional risk management practices are labor-intensive and time-consuming, where businesses and organizations rely on historical data and tedious systems to identify potential threats. With the accelerating pace of threats, it is evident that a more proactive and adaptive approach is required, where AI would become especially relevant in risk assessment. The Institute for Defense Analyses writes: “One important way in which emerging technologies such as AI and ML should be useful is in cutting through the volume of data and finding indicators of compromise using correlations across data sources. These systems would assist human analysts by elevating or alerting them to significant events that require responses without overwhelming the organization with false alarms or other spurious indicators.” (Loaiza 9) Of course, with the implementation of new technologies, it is necessary to ensure the protection of sensitive data while upholding the performance of advanced algorithms. With this in mind, one of the primary advantages of AI in risk management is its capacity for proactive threat detection- AI models could analyze current data and patterns to identify emerging risks. The shift from reactive to proactive threat detection would be a fundamental development from conventional risk management approaches and would give organizations the capability to stay ahead of cyber adversaries. These systems would increase the efficiency in detecting threats and minimize false positives by learning to distinguish normal and anomalous behavior over time.

The aforementioned automation and efficiency that AI provides would allow organizations to allocate their human resources elsewhere. Routine tasks such as data collection, analysis, and reporting can be automated through AI systems which would not only accelerate

the risk assessment process but reduce the presence of human error. The *National Artificial Intelligence Research and Development Strategic Plan* states that: “AI technologies can maximize efficient use of bandwidth and automation of information storage and retrieval. AI can improve filtering, searching, language translation, and summarization of digital communications, positively affecting commerce and the way we live our lives.” (Haugh 20) For instance, in the event of a security risk, AI automation facilitates a more efficient and precise response. Automated response systems can promptly analyze and categorize incidents, prioritize based on severity, and execute predefined responses if necessary. Tim Stevens articulates the significance of automating certain tasks: “The collection and filtering of data about the status of information systems and threats to their intended functioning have long been largely automated. Humans do not have the cognitive or sensory capacity to cope with the enormous data volumes produced by software and hardware dedicated to alerting systems administrators to problems inside and outside their networks. Add to this a human capital shortfall in the cybersecurity industry (Shires 2018) and automation is a reasonable technical fix for some of these problems.” (Stevens 1) These systems not only reduce response time but also ensure consistent and controlled responses to security risks. The potential of AI allows the *National Artificial Intelligence Research and Development Strategic Plan* to make certain assumptions that support AI’s future in risk management:

> “First, it assumes that AI technologies will continue to grow in sophistication and ubiquity, thanks to AI R&D investments by government and industry. Second, this plan assumes that the impact of AI on society will continue to increase, including on employment, education, public safety, and national security, as well as the impact on U.S. economic growth. Third, it assumes that industry investment in AI will continue to grow, as recent commercial successes have increased the perceived returns on investment in R&D. At the same time, this plan assumes that some important areas of research are unlikely to receive sufficient investment by industry, as they are subject to the typical underinvestment problem surrounding public goods. Lastly, this plan assumes that the demand for AI expertise will

> continue to grow within industry, academia, and government, leading to public and private workforce pressures." Pg. 6

The capabilities of AI in risk management are evident, so naturally its potential in cybersecurity frameworks must be acknowledged. The use of AI to improve compliance management in cybersecurity models such as CMMC and NIST 800-171 would ensure adherence to regulatory requirements. Because AI excels at automating the monitoring of cybersecurity controls, with continuous assessment and reporting, organizations can reduce the manual effort required for audits and ensure a proactive stance toward compliance.

AI Risks and Limitations

Before formally discussing cybersecurity frameworks and their future with AI, understanding the risks and limitations of new technologies is vital. One of the more prominent risks of utilizing AI in cybersecurity is its vulnerability to adversarial attacks, which involve the manipulation of data to deceive AI systems into generating incorrect results. This issue can be exploited by altering data inputs, thus leading AI to misclassify threats or overlook certain vulnerabilities. A literature review on *The Impact and Limitations of Artificial Intelligence in Cybersecurity* notes that: "One of the most significant limitations of AI is that it is just a computer code programmed to ensure that they have followed the protocols and developed themselves in case of anything…the system is entirely programmed; therefore, anybody can take control of them, and they can be manipulated and used as a weapon." (Ansari 87) Evidently, this risk poses a significant obstacle in proving the reliability of AI-driven cybersecurity measures, necessitating a substantial amount of research and development into these systems to avoid these attacks. Relating, because of the extensive data utilization required in the integration of AI, there are issues concerning data privacy and security. The reliance on automation and AI's ability to store extensive amounts of data poses a threat of potential breaches and unauthorized access to

sensitive information. And, since these models require comprehensive datasets to work effectively, there are concerns regarding the anonymization and security of data.

Of course, with the evolution of cyber threats, the potential for false positives or negatives in automated threat detection leaves the possibility of unintended consequences that could compromise the overall security posture. An overreliance on AI for threat detection might trigger unnecessary alerts and responses, or, conversely, an oversight of a model's training data might result in actual threats being overlooked. In other words: "AI systems are generally empowered to make deductions and decisions in an automated way without day-to-day human involvement. They can be compromised, and that can go undetected for a long time." (Goosen 2) Because of the nature of AI, there are some obstacles involving its adaptation to newer cyber-attack tactics. The rapid development of new threats calls for continuous improvements to AI algorithms to ensure their effectiveness in identifying attack methodologies and emerging threats. For one, keeping AI models up to date with relevant issues requires continuous monitoring, threat intelligence integration, and consistent system updates. A proactive and collaborative approach is fundamental to fully leverage the potential of AI in cybersecurity.

AI's interaction with humans also brings certain considerations into play, such as the ethical considerations and algorithmic bias within these systems or the lack of transparency in artificial models. These algorithms have the possibility of presenting bias toward or against individuals or groups, leading to disparities in threat detection and response through inadvertent discrimination. For example, an AI system may exhibit bias in recognizing certain types of cyber threats, potentially overlooking specific attack vectors that disproportionately affect certain demographics. The *National Artificial Intelligence Research and Development Strategic Plan* addresses this issue as well:

> "Ethical issues vary according to culture, religion, and beliefs. However, acceptable ethics reference frameworks can be developed to guide AI system reasoning and decision-making, in order to explain and justify its conclusions and actions. A multi-disciplinary approach is needed to generate datasets for training that reflect an appropriate value system, including examples that indicate preferred behavior when presented with difficult moral issues or with conflicting values. These examples can include legal or ethical "corner cases", labeled by an outcome or judgment that is transparent to the user. AI needs adequate methods for values-based conflict resolution, where the system incorporates principles that can address the realities of complex situations where strict rules are impracticable." Pg.27

Clearly, addressing algorithmic bias in an artificial system requires significant efforts and implementation of training data to identify and avoid existing prejudices. Regarding AI's lack of transparency, this problem stems from AI's deep learning algorithms and the complexity of their systems, which require multifaceted interpretations of the results they provide. When AI is utilized for cybersecurity measures, it often raises questions as to why or how the system reached particular decisions or identified potential threats. The issue here involves the relationship between these systems and human professionals, and how the opacity of AI-generated conclusions may undermine the capabilities and predisposed knowledge of the latter. Consistent testing and evaluation of these systems is necessary to create reliable and easily understandable results, allowing for a "trustworthy" and transparent user experience.

Regulation of AI

By acknowledging the risks and limitations in utilizing AI one must ask how to properly regulate these issues, so as to guarantee the safety and ethicality of AI systems while subsequently employing their potential. A primary element in AI regulation involves defining clear objectives or finding the balance between fostering innovation and mitigating risk. To avoid the issues discussed above, it is useful to define objectives that encompass the transparency of AI, meaning they should address bias issues and maintain boundaries between human control and the

autonomy of AI. These boundaries ensure the clarity of artificial systems, allowing human professionals to understand their decision-making processes, which facilitates the validation and trustworthiness of these systems. Chris Reed argues that: “The obvious regulatory response is to require each AI tool which has the potential to infringe fundamental rights to be able to explain the reasoning leading to the tool’s decisions.” (Reed 3) Of course, with transparency comes accountability, where determining responsibility in the event of a security incident or failure becomes crucial. This practice fosters the continuous development and improvement of AI systems, allowing developers to monitor and react accordingly to the performance of artificially driven cybersecurity measures.

As previously discussed, the ethicality and human relationship with AI in cybersecurity is a significant concern to be addressed. Regulative measures should encompass guidelines for the ethical utilization of data, ensuring that AI systems adhere to privacy rights and avoid discriminatory practices. Given the global nature of cyber threats, AI regulation in cybersecurity requires international cooperation and an understanding of common standards. As such, it should be mandatory that regulatory frameworks promote the responsible development and deployment of AI in the cybersecurity domain, to avoid potentially global conflicts. This is where the relationship between human oversight and AI becomes essential; regulatory frameworks should define the boundaries where AI systems can autonomously make decisions and where human intervention is necessary. Finding the proper balance between the two would prevent unethical practices, inasmuch as is humanly possible. The synergy between human understanding of ethicality and the artificial capabilities of AI would promote innovation without compromising morals.

Compliance Audits and their Relationship with Cybersecurity Frameworks

An applied solution to regulating AI involves audits or mechanisms for compliance verification. Regular assessments of AI systems in cybersecurity, conducted by external entities, would promote adherence to regulatory standards. For example, a compliance audit is an independent examination to determine whether an organization is adhering to specific laws, regulations, or internal policies and procedures. This way, an organization's activities may be assessed to determine their alignment with established requirements. Key characteristics of a compliance audit include:

• Objective Evaluation
○ Compliance audits are conducted externally to ensure impartial judgment of the organization's compliance with laws, regulations, policies, contractual obligations, or internal policies
• Scope Definition
○ The scope of these audits is defined based on the regulations that an organization is expected to comply with. This scope may include legal, financial, operational, or information security aspects
• Examination of Processes
○ This involves the examination of the organization's internal controls, processes, and documentation to ensure compliance
• Documentation Review
○ Auditors review relevant documentation to verify alignment with compliance standards
• Testing and Verification
○ Auditors may conduct testing to verify the implementation and effectiveness of controls and procedures. This may involve sample testing of transactions, processes, or data
• Identification and Report of Non-Compliance
○ Deviations from compliance requirements are documented and included in a report that outlines findings, including areas of compliance and non-compliance

Compliance audits are crucial in promoting the transparency and effectiveness of an organization's processes, such as their use of AI systems. They assure stakeholders that the

organization is complying with the regulatory standards that they are expected to adhere to. Compliance audits also possess an intricate relationship with cybersecurity frameworks such as CMMC and NIST 800-171 in that the former assesses the implementation of the standards provided by the latter. For example, to achieve CMMC certification, businesses and organizations must undergo assessments conducted by certified third-party assessment organizations (C3PAOs). Similarly, NIST 800-171 compliance is assessed through third-party audits to validate their compliance with regulatory guidelines and requirements.

How AI Can Improve CMMC/NIST Compliance

AI finds substantial relevance in cybersecurity, particularly in intrusion detection systems. Traditionally, cybersecurity solutions primarily conducted traffic analysis to classify internet traffic as either legitimate or malicious and would rely on rule-based systems and signature-based detection. An applied example of AI's practicality involves its detection of false information: "False information can seriously affect both national security and people's wellbeing; and detecting false information has become a modern application-layer cybersecurity issue. AI has proven to be a versatile technique to detect false information, as it can quickly analyze a large amount of data. For example, in, the authors analyzed a corpus of 11,000 articles, including news from Reuters, local news, and blogs, and about 29 percent of articles of the corpus were labeled as fake. Their work classified fake news with 77.2 percent accuracy using Stochastic Gradient Descent, an iterative optimization algorithm." (Zeadally 11) Furthermore, with the expansion of connected devices and applications, the increasing volume of network traffic made the development and rules for analysis cumbersome and resulted in the creation of defensive rather than proactive security measures. Concurrently, technological advancements allowed individuals conducting cyberattacks to develop increasingly sophisticated strategies,

challenging the safety and capabilities of existing security systems. Naturally, with AI's capacity to analyze and classify large volumes of data, it emerges as a potent solution with its ability to automate attack detection and its continuous evolvement in response to developing cyber threats. As CMMC and NIST 800-171 are heavily centered around requiring organizations to uphold robust cybersecurity standards, the application of AI systems would play a crucial role in enhancing the level of cybersecurity.

Deep Learning algorithms are a type of AI that excels in automated threat detection, which remains an integral part of complying with CMMC and NIST 800-171. By leveraging these algorithms, organizations can conduct in-depth risk assessments that are tailored to align with the requirements of their respective cybersecurity framework. For example, AI can dynamically create compliance roadmaps based on an organization's specific needs, while correspondingly considering factors like industry, size, and level of protection their data requires. This adaptability ensures that AI's enhancement of compliance is relevant to a variety of organizations and can adjust accordingly, promoting inclusivity. Additionally, AI's continuous monitoring ability allows for real-time updates on any modifications made to CMMC or NIST 800-171 guidelines. This way, organizations can promptly make the necessary changes based on the interpretations of best practices provided by AI systems. Its predictive analysis can anticipate future updates made to CMMC and NIST 800-171, allowing organizations to proactively prepare for compliance requirements. These compliance requirements are typically listed in lengthy documents; however, AI-driven tools have the capability to streamline time-consuming documentation processes.

There are numerous and ever-developing examples of how AI can specifically function according to different situations. In addition to the discussed automated threat detection, certain

AI systems enable deep packet inspection, which ensures the integrity of data transmitted and received. This is because "…the issues in data acquisition (amount, heterogeneity, and velocity of data) as well as the problems of the related tools (low detection rate, slow throughput, lack of scalability and resilience, and a lack of automation) could be mitigated through AI." (Wirkuttis 7) This assures the adherence to NIST 800-171's requirements relating to data protection and confidentiality. AI also enables another level of data security which involves the latter's classification and encryption, categorizing information based on content and context, further enhancing compliance with security requirements. Moreover, CMMC and NIST 800-171 both emphasize user activity monitoring in their compliance requirements, and certain AI algorithms can analyze user behavior patterns. Through continuous analysis and learning, these systems can detect anomalies, such as unauthorized access to sensitive information or generally suspicious activity. For example, Deep Learning algorithms can process multimodal data, incorporating diverse types of information such as packet headers, payload content, and network behavior. This allows for a more holistic understanding of network activity and differentiation between normal and malicious activity concerning Denial of Service (DoS)[1] attacks. This same pattern recognition ability can be applied to access control mechanisms which, by understanding the patterns of authorized user access, AI can determine whether or not access permissions align with policies listed in cybersecurity frameworks. Overall, the incorporation of AI would decrease human involvement in cybersecurity, which remains a vulnerable element due to its fabrication of human error. Adaptability and proficiency in handling complex cybersecurity issues make AI a valuable factor for organizations to proactively comply with CMMC and NIST 800-171 standards.

[1] A DoS attack involves the disruption of the functionality of a network, service, or website by overwhelming it with a vast number of illegitimate requests or traffic. The primary goal of these attacks is to render the target system or network unavailable to its intended users, causing a denial of service.

Conclusion

Through examining the relationship between AI and cybersecurity frameworks such as CMMC and NIST 800-171, it is clear the implementation of AI systems into cybersecurity has become progressively more necessary, especially with the ever-developing cyber threats and vast amounts of transmitted data. However, it is vital to acknowledge the inherent risks and limitations of AI, and the need for ongoing research and monitoring when integrating AI into cybersecurity practices. Boundaries must be made to ensure the ethical deployment of these systems, especially when mitigating unwanted bias or discrimination toward certain groups of people. These boundaries hinder the possibility of potentially global issues arising, due to the international and electronic transmission of data. Nonetheless, with the proper execution and observation of AI systems, organizations can proactively respond to cybersecurity requirements outlined in frameworks such as CMMC and NIST 800-171. Compliance with these requirements prominently benefits organizations, introducing them to many contractual and competitive opportunities.

Looking ahead, there are many prospects for further exploration of this topic. For example, one may research the different types of cyber threats and begin understanding the corresponding AI systems to address specific issues. Differentiating AI applications tailored to diverse types of cyberattacks, from phishing attacks to ransomware, would provide an even more pronounced understanding of AI's versatility. Other areas for potential further examination include how AI can contribute to identifying security issues during the development lifecycle (relating to following secure coding principles), AI simulations or training modules to promote cybersecurity awareness, or even how AI strategies can facilitate collaboration across different industries. Continuous advancements in AI and the dynamic nature of cyberattack techniques

allow for invigorating and ongoing exploration of AI-driven solutions to ensure their effectiveness and utility.

References

Andy Marker. “The Official Guide to Compliance Auditing.” *Smartsheet*, smartsheet.com/compliance-auditing. Accessed 29 Nov. 2023.

Ansari, Meraj Farheen, et al. “The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review.” *SSRN*, 13 Jan. 2023, papers.ssrn.com/sol3/papers.cfm?abstract_id=4323317.

Braw, Elisabeth. AI and Gray-Zone Aggression: Risks and Opportunities. American Enterprise Institute, 2023. JSTOR, http://www.jstor.org/stable/resrep52271. Accessed 29 Nov. 2023.

“Compliance Audit Basics: Definition, Types, and What to Expect.” *AuditBoard*, www.auditboard.com/blog/compliance-audit/. Accessed 29 Nov. 2023.

Gamble, William. *The Cybersecurity Maturity Model Certification (CMMC) - A Pocket Guide*. IT Governance Ltd, 2022.

Goosen, Ryan, et al. “Artificial Intelligence Is a Threat to Cybersecurity. It’s Also a Solution.” *BCG Global*, BCG Global, 15 Sept. 2022, www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.

Green, Matt. “Conducting a Compliance Audit.” *Skillcast*, www.skillcast.com/blog/conduct-compliance-audit. Accessed 29 Nov. 2023.

Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity, ieeexplore.ieee.org/document/8963730. Accessed 29 Nov. 2023.

Haugh, Brian A., et al. “Appendix B.: The National Artificial Intelligence Research and Development Strategic Plan.” RFI Response: National Artificial Intelligence Research and Development Strategic Plan, Institute for Defense Analyses, 2018, pp. 15–64. JSTOR, http://www.jstor.org/stable/resrep22865.11. Accessed 29 Nov. 2023.

Inss.Org.Il, www.inss.org.il/publication/artificial-intelligence-cybersecurity/. Accessed 29 Nov. 2023.

Loaiza, Francisco L., et al. Utility of Artificial Intelligence and Machine Learning in Cybersecurity. Institute for Defense Analyses, 2019. JSTOR, http://www.jstor.org/stable/resrep22692. Accessed 29 Nov. 2023.

Manyika, James. “Getting AI Right: Introductory Notes on AI & Society.” Daedalus, vol. 151, no. 2, 2022, pp. 5–27. JSTOR, https://www.jstor.org/stable/48662023. Accessed 29 Nov. 2023.

Reed, Chris. “How Should We Regulate Artificial Intelligence?” Philosophical Transactions: Mathematical, Physical and Engineering Sciences, vol. 376, no. 2128, 2018, pp. 1–12. JSTOR, https://www.jstor.org/stable/26601758. Accessed 29 Nov. 2023.

Tabassi, E., & Tabassi, E., Artificial Intelligence Risk Management Framework (AI RMF 1.0).

United States, Congress, Ross, Ron, et al. *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

United States, Congress, Tabassi, Elham, and Elham Tabassi. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*.