AI-Enhanced Cybersecurity Solutions for Protecting U.S. Aerospace Manufacturing Infrastructure: Techniques and Real-World Applications

By Dr. Ayşe Gülcü

Professor of Electrical and Electronics Engineering, Istanbul University, Turkey

1. Introduction

The aerospace manufacturing infrastructure of the U.S. has been a target of cyberattacks by nation-states and hackers attempting to poach its intellectual property. Cyberattacks are conducted to compromise the confidentiality, integrity, or availability of computer systems and networks. They are exploited via malware, distributed denial of service attacks, exploiting vulnerabilities, and human errors. Cyberattacks can have severe consequences on the attacked systems, creating economic vulnerabilities for the affected entities. A federal sUAS acquisition directive was enacted to strengthen the cybersecurity posture of contractors that provide systems with software components that could be exploited with malware during the electronic supply chain. Current cybersecurity solutions rely on the use of rules-based systems and threat intelligence feeds to detect cyberattacks. To augment such defensible architectures in U.S. aerospace manufacturing infrastructure of interest, AI-enhanced network intrusion detection systems are reviewed for potential application. The research stage of the supply chain security architecture is detailed and a literature review is conducted. Four AI-enhanced cybersecurity solutions, supported by published proof-of-concept and research prototypes, are examined. Each implementation would operate independently or could be seamlessly integrated into a layered approach to covering attack vectors associated with reconnaissance, exploitation, and installation levels of the cyber kill chain [1] , [2].

The U.S. aerospace manufacturing infrastructure seeks to prevent and take action against cyberattacks on a plant network. The problem of network cybersecurity is framed in the context of supply chain security adapted to manufacturing. Intentional corporate espionage cyberattack vectors, tactics, techniques, and procedures, or MITRE ATT&CK, are informed and adjusted for the supply chain security context. AI-based approaches for intrusion detection, deception generation, and data exfiltration environment emulation are separately

This work is licensed under CC BY-NC-SA 4.0.

framed, reviewed for their potential application, and further proposed for research and development.

1.1. Background and Significance

The international aerospace manufacturing industry is highly competitive, complex, and technologically challenged. Manufacturing processes involve highly sensitive technologies and proprietary manufacturing processes. The increasing number of cyberattacks on aerospace manufacturing sectors is a concern and threat that needs to be addressed. Nation states have an interest in acquiring or disrupting technologies that would negatively impact U.S. industries' competitive advantage. Today's interconnectedness of manufacturers and supply chains has fuelled a renewed call to protect from state-sponsored or financially motivated espionage and cyberattacks. Manufacturing technologies sensitive to intellectual property theft or sabotage must be adequately protected to prevent negative impacts on the lives of U.S. citizens [2].

Emerging artificial intelligence (AI) capabilities offer great promise in preventing cyberattacks from impacting manufacturing and assembly systems. Understanding how AI can be an integral component of cybersecurity solutions requires knowledge of existing and emerging manufacturing technologies. The objective is to review AI-enhanced cybersecurity solutions for protecting the U.S. aerospace manufacturing industry's intellectual property [1]. Specific manufacturing technologies of focus are either additive or subtractive aerospace manufacturing. Specifically, the manufacturing of complex 3D geometries and sensitive aerospace components through directed energy deposition additive processes, as well as five-axis CNC hermetic machining, are discussed. Understanding manufacturing technologies and cyberattacks of concern aids in identifying AI-enhanced cybersecurity solutions and illustrating real-world case studies of implementations.

1.2. Research Objectives and Scope

The escalating frequency and sophistication of cyberattacks targeting Critical Infrastructure (CI) pose significant threats to national security and safety. In response to broadening cyber threat vectors, the government must provide the Cybersecurity and Infrastructure Security Agency (CISA) with broad new authorities to address vulnerabilities proactively and

This work is licensed under CC BY-NC-SA 4.0.

comprehensively across all sectors [3]. Additionally, national strategies should center on Natural Language Processing (NLP) and Big Data processing capabilities while appropriate resources are allocated to overcome the emerging technologies gap with adversarial nations. Given the aforementioned, AI-enhanced cyber solutions are proposed to protect U.S. aerospace manufacturing infrastructure. AI is already being adopted in the defense sector, including aerospace manufacturing. Promising civilian use cases exist with opportunities to inform a similar understanding of AI in the national security realm [4].

The objective of this research is to explore how AI-enhanced cybersecurity solutions can protect U.S. aerospace manufacturing infrastructure. In alignment with the overall research topic, the specific objectives of this study involve (i) exploring U.S. aerospace manufacturing infrastructure and its use cases and application of AI-enhanced cyber solutions, and (ii) exploring industry benchmarks for building enterprise resilience using AI and other emerging technologies. Within this context, discussions can then occur in the broader realms of (iii) U.S. government, Department of Defense, Office of the Undersecretary of Defense for Research and Engineering cybersecurity maturity framework, and (iv) specific recommendations for manufacturers and CISA. The overarching goal is to construct a detailed understanding of U.S. aerospace manufacturing infrastructure use cases involving AI-enhanced cyber solutions to inform a recommendation framework.

2. Cybersecurity Threats in Aerospace Manufacturing

The National Institute for Standards and Technology (NIST) defines critical manufacturing industries as those that may have a significant impact on national security or other essential interests. The aerospace manufacturing sector belongs to this category because of the industrial base that supports the maintenance of well-functioning commercial and defense industries. This sector is a critical part of the infrastructure that supports technology leadership, provides sustainable economic opportunities, and contributes to the nation's safety and security.

Aerospace services must have the highest level of trust and reliability involving critical aircraft functions and safety-sensitive systems, warfighter advantages, advanced military security, satellite processing, and global communication linkages, including complex related production activities. The overarching nature of these security and safety characteristics

This work is licensed under CC BY-NC-SA 4.0.

makes the entire global aerospace enterprise an extremely attractive target for a wide variety of advanced attacks designed specifically to compromise aerospace systems.

What makes aerospace manufacturing especially challenging in terms of attacks is that it is the ultimate accumulation of the complexity of a multi-tiered global supply chain that couples relatively few original equipment manufacturers (OEM) with multiple layers of suppliers of unknown and not always well-studied integrity.

The traditional approach to cybersecurity provides security from a fixed perimeter and assumes that attackers using the internet should be kept off the internal networks. This approach is ineffective because traditional attack paths are no longer the critical threat vectors, and they have trouble scaling with the speed of new adversaries. There is a severe threat that the massive amounts of financial, human, and intellectual capital being spent to secure critical systems might not achieve the overall concept of defense in depth needed to protect those systems from contemporary threat vectors.

Attacks have moved up from the silicon substrate to the software surface visible to and accumulating the financial investments of the aerospace manufacturing industry. With the heavy capital investment in model-based systems engineering (MBSE) and the digital thread of computer-aided design (CAD), finite element analysis (FEA), and computer-aided manufacturing (CAM) systems, the entire aerospace manufacturing production process is powered by complex software systems. The possibility of leaving these attractive sandboxes open to determined and intelligent adversaries looking to leverage advanced counterfeiting, theft, or functional manipulation of the host systems cannot be dismissed.

The traditional approach to cybersecurity is being replaced by some implementing artificial intelligence (AI) and deep learning (DL) technologies. These technologies protect our nation's critical infrastructure that powers modern technical capabilities. In recent years, the use of AI to augment traditional cybersecurity approaches has been rapidly gaining attention. The gap between effective attack and defense is steadily widening, and the exploitation of readily available advanced technologies is accelerating this process.

It is needed to take a step that goes beyond simply improving the integration and implementation of given traditional security and move to AI-enhanced systems that

This work is licensed under CC BY-NC-SA 4.0.

comprehensively harden the resulting frameworks against modern, intelligent adversaries. This paper discusses how AI and its derivative technologies can be used to augment existing aerospace manufacturing systems and services and consider the steps that must be taken to ensure that AI-based security systems are always effective, resilient, easy to challenge, and hard to scale.

2.1. Overview of Cybersecurity Threat Landscape

[3][2] Building upon the previous section, the following specifics of the cybersecurity threat landscape are presented. In particular, the complexities and challenges posed by cyber threats to aerospace manufacturing are articulated to set the stage for the presentation of specific threats in the following section. Cyber threats have evolved significantly in the past two decades owing to rapid advancements in technology and the global proliferation of computer networks. Cyber threats consume enormous resources in terms of time, money, and security efforts, with significant effects on both industries and nations, primarily in the United States (U.S.). Aerospace manufacturing involves complex equipment, hardware, and electronically controlled systems. The aerospace industry significantly contributes to the U.S. economy and is critical to national security in terms of defense capabilities. Cyber threats to the aerospace sector can compromise system availability, integrity, and confidentiality. Cyber incidents can have an even wider impact on the entire economy vis-a-vis international competition. Aerospace manufacturing is at higher risk for countries without a deep scientific/engineering base, and threats are not always external; they can emanate from manufacturers with sensitive information, contractors that supplement/manufacture components, staff co-op and internship programs, partnerships with academic institutions, foreign acquisitions.

2.2. Specific Threats to Aerospace Manufacturing

The aerospace manufacturing industry is comprised of complex manufacturing processes that combine intricate designs and unique materials. These components have stringent reliability standards since failures could endanger lives and/or costly systems. Aviation systems exude a high availability demand and operate continuously for prolonged periods of time while thoroughly monitored for failure and performance. These manufacturing processes are currently undergoing a transformation that embraces advanced digital technologies under an integrated approach, known as the Fourth Industrial Revolution or Industry 4.0 [5]. In

This work is licensed under CC BY-NC-SA 4.0.

addition to the historical manufacturing capabilities, data collection sensors and manufacturing tools are being added to the ecosystem and providing more insight on processes. Manufacturing systems are statistically analyzed and monitored to prevent faults and/or preventively schedule maintenance. Although the Industry 4.0 paradigm provides newly available data and has the potential to improve the aerospace manufacturing processes significant amounts, it also exposes manufacturing systems to cybersecurity vulnerabilities. As with any Industry 4.0 ecosystem, aerospace manufacturing systems consist of complex networks of connected "smart" cyber-physical entities that propose a unique set of threats.

Aerospace manufacturing processes are commonly comprised of individual machines that perform specialized tasks on the workpiece and are heavily automated. This automation enhances consistency, productivity, and reliability levels in comparison to conventional manual machining processes. However, since those processes involve supervised human-machine interaction, they execute a set of commands or set points based on pre-defined trajectories. Those settings are modified to recover from tooling wear while maintaining quality and efficiency metrics. Adding these multi-domain signals, whether within controllers or through integration, elevates the future threat postures [6]. The control inputs effectively create a physical bridge to the workpiece and expose a direct method to compromise the integrity of aerospace components produced in the manufacturing system.

3. Fundamentals of Artificial Intelligence in Cybersecurity

Artificial intelligence (AI) is a term for different types of technologies that give machines the ability to show intelligence comparable to that of a human being. These technologies give machines the ability to show intelligence comparable to that of a human being using capabilities, such as reasoning, learning, problem solving, decision making, perception, and understanding of human communication (written and spoken language). There are different types of AI technologies, which can be categorized into narrow or general AI. Narrow AI means that a machine has human-level intelligence for a narrow task. For example, systems that can beat the best chess player in the world have narrow AI. General AI means that a machine has human-level intelligence across a broad range of disciplines. There is currently no machine that has general AI [7].

This work is licensed under CC BY-NC-SA 4.0.

An innovative approach for developing AI is to imitate the structure and function of the human brain and its neurons. This idea forms the basis for artificial neural networks, which consist of many simple units (nodes), each of which is connected with a strength (weight) to other units. Each of the units sums its weighted inputs and has an activation function that determines how much influence the unit has on the network's behavior. Feedforward neural networks, which are the simplest kind of neural networks, can be used for classifying data into multiple categories. Other more complex architectures of neural networks have been developed for more sophisticated tasks, including recurrent neural networks with in-memory feedback connections for processing sequential data and deep learning networks with multiple hidden layers. Deep learning systems uncovered the spectacular recognition abilities of different forms of data in real time [2].

3.1. Machine Learning and Deep Learning Basics

Integrating AI technologies to create innovative approaches for detecting and mitigating "Known" and "Unknown" cybersecurity threats, as deeper insights into these advanced technologies successfully dealing with cybersecurity challenges are summarized. The following sections provide a holistic view of the topics leveraged to tackle the innovation problem. As an initial step of germination, the fundamentals of machine learning and deep learning are dissected to achieve a fundamental and comprehensive understanding of these key technologies and their relevance to cybersecurity. The gathered knowledge is utilized to analyze the capabilities of machine learning techniques before providing an overview of related real-world applied projects and research activities in the domain of advanced machine learning-aided cybersecurity. The main goal is to delineate a proposed holistic solution space of AI-enhanced cybersecurity capabilities targeting the overall problem domain of the U.S. aerospace manufacturing infrastructure with its interrelated and consequential challenges. This solution space consists of several advanced techniques, some of which are already prototyped and certified, while others are still in the research phase but hold significant promise [2].

Machine learning is the scientific study of algorithms and statistical models that computer systems use to perform tasks without explicit instructions. It is widely applied and is a key component of artificial intelligence. As part of data science, machine learning is closely related

This work is licensed under CC BY-NC-SA 4.0.

to the fields of statistics, optimization, data mining, and pattern recognition. A set of data comprising training examples is used to teach a machine learning system to make predictions. The data can be labeled, where the correct outputs are known, or unlabelled, where the system must find outputs on its own [7].

3.2. Applications of AI in Cybersecurity

AI technologies can play a crucial role in the detection and mitigation of cyber threats. As the aerospace manufacturing domain becomes increasingly automated, AI-augmented solutions are needed to bolster current cybersecurity defenses. AI solutions can address cyber threats in (1) continuous monitoring of system architectures and software components, (2) fugitive malware detection, (3) network intrusion detection, and (4) insider threat detection [3]. All four of these threat vectors threaten the integrity of a company's manufacturing production and could provide adversarial agents with critical intellectual property. System architectures are monitored through the continuous analysis of the output of program analysis techniques and the continuous execution of vulnerability monitoring techniques. Analysis of software components includes the monitoring of vulnerable or outdated software libraries, which allows a company to be notified of potential system vulnerabilities and for current vulnerabilities to be remediated quickly. Recognizing anomalous changes in software components or unintended software changes within component updates is also monitored. Focusing on fugitive malware, indicators of compromise occurring from malware executing on physical hardware or software components can be detected in monitoring environments [1]. The outputs from honeypots, also known as failure environments, are maintained to monitor attempts to breach security protocols, analyze the tactics, techniques, and procedures (TTPs) being used by attackers, and develop signatures or indicators of suspicion based on the monitoring of these attempts.

4. Integration of AI in Cybersecurity for Aerospace Manufacturing

This section explores the integration of both AI and ML into cybersecurity measures that are tailored to protect aerospace manufacturing infrastructure. There are challenges, as well as opportunities, associated with the incorporation of AI-driven cybersecurity solutions into the unique cybersecurity landscape of the aerospace manufacturing industry [1]. The current state of conventional cybersecurity controls within aerospace manufacturing operations is first

This work is licensed under CC BY-NC-SA 4.0.

examined, followed by an outline of how AI technologies can be specifically applied to enhance these existing controls.

The primary intention of this section is to provide a simple roadmap of the process of firmly positioning AI in cybersecurity efforts focused on aerospace manufacturing. Notable examples of real-world applications of AI in cybersecurity for the aerospace manufacturing industry are also provided to illuminate the path forward. Defense-in-depth is a commonly employed term in business cybersecurity programs meaning that there are multiple levels of protection implemented against potential cyber threats [2]. Organizations in the aerospace manufacturing space typically deploy a variety of conventional cybersecurity controls to steadily prevent, detect, and respond to cyber threats.

4.1. Challenges and Opportunities

Understanding the challenges that need to be addressed before AI could be broadly utilized in supporting cybersecurity in aerospace manufacturing is important to ensure there is adequate research being performed in these areas. In a review of state of the art AI research, Sarker et al. identified several important challenges that must be overcome: lack of trust, data quality issues, and diversity of attack modes. Trusted-trained AI algorithms must produce consistent outputs. Trends indicate that trust is declining in AI models. Actively building trust with users via transparency, accessibility, and accountability is essential. Quality and integrity of training data is vital, higher quality (well documented and contextualized) data increases model trustworthiness [8]. AI algorithms must maintain an up-to-date adaptable model that handles new cyber attack modes as they arise. Well-trained AI models can still fail if not sufficiently trained on all relevant attack modes. AI models must be globally diverse, to anticipate how different cultures use innovative technology. Otherwise, biased models may fail to adequately address a new attack mode in a different culture. In the aerospace manufacturing domain, common approaches such as reporting trends and volumes of attacks experienced offers a limited view of threats encountered, preventing attack mode diversity from being drawn from multiple industry perspectives.

In creating AI-enhanced cybersecurity, there are opportunities in improving the efficiency of training data generation and increasing diversity by re-utilizing collected data from multiple companies. Actively meeting compliance audit requirements requires extensive data

This work is licensed under CC BY-NC-SA 4.0.

documentation. The creation of both AI and diverse datasets to easily show compliance would naturally collect important documentation and metrics (with the potential to avoid data protection issues). Publicly available, labeled images of hardware with security vulnerabilities would aid AI algorithms, like those in self-driving cars, to match video feeds to know attack vectors (e.g. physically exploiting an ethernet port). While there are significant aspects of AI in the aerospace manufacturing environment, addressing the aforementioned set of challenges with aerospace-industry-oriented techniques creates an opportunity for researchers to help close the gap of potentially compromised systems.

4.2. Benefits of AI in Aerospace Manufacturing Cybersecurity

The complexity and sophistication of cyberattacks have been progressively increasing. Therefore, cybersecurity strategies have been optimized to provide the most coverage possible against attacks and incidents. Nevertheless, it is inevitable that systems will be violated and, in these events, an automatic and effective response is required to manage the situation and minimize collateral damage. Recently, there has been greater awareness of the possibility of using AI-based systems to meet these requirements, but there remain many open questions, particularly concerning the epistemic side [3].

In the past decades, organizations have been pushed towards the implementation of automation systems that aim to reduce operational costs. New technologies, such as the IoT and industrial control systems, have been deployed across many industries to achieve this goal. However, the development of these technologies has also opened up new entrance points for vulnerabilities, and therefore cyberattacks, in critical infrastructure. In particular, automated control of systems implies that reliable information should be collected and processed to make appropriate decisions. This makes industrial systems easier to violate as the deception and spoofing of collected data will lead to a productive effect on the control system, resulting in the accomplishment of pre-specified objectives.

5. Real-World Applications of AI-Enhanced Cybersecurity in Aerospace Manufacturing

AI-enhanced cybersecurity solutions have been successfully employed in various aerospace manufacturing applications to protect sensitive data and systems from cyber threats. One notable case study involves Northrop Grumman, a leading aerospace and defense technology

This work is licensed under CC BY-NC-SA 4.0.

company, which implemented AI-powered cybersecurity solutions to monitor and analyze network traffic for potential threats. By leveraging machine learning algorithms to establish a baseline of normal behavior, Northrop Grumman was able to detect anomalies in real time and respond to potential attacks more effectively.

Another example is the integration of AI-enhanced cybersecurity systems within the supply chain of aerospace manufacturers. With the increasing interconnectivity of suppliers and manufacturers, new vulnerabilities arise, making it essential to extend cybersecurity measures beyond the organization's own systems. Lockheed Martin collaborated with a consortium of aerospace manufacturers to develop an AI-powered cybersecurity framework that shares threat intelligence and best practices across the supply chain, improving the overall security posture of the industry.

In a different approach, a small aerospace manufacturer specializing in unmanned aerial systems partnered with a cybersecurity firm to assess and strengthen its cybersecurity controls. The firm conducted penetration testing and vulnerability assessments, uncovering critical vulnerabilities in the company's network and systems. They then worked together to remediate these vulnerabilities and implement AI-driven solutions for continuous monitoring and threat detection.

In summary, AI-enhanced cybersecurity solutions have been effectively deployed in real-world aerospace manufacturing applications, protecting sensitive data from cyber threats. These case studies highlight the potential and success of AI in addressing cybersecurity challenges within the aerospace manufacturing sector [2].

5.1. Case Studies and Success Stories

Focusing specifically on case studies and success stories, in-depth analyses of real-world applications of AI-enhanced cybersecurity in aerospace manufacturing are presented. Aims to draw insights from actual implementations and their outcomes, highlighting the effectiveness of AI in addressing cybersecurity concerns.

Innovation in AI and machine learning (ML) provides the potential for significant improvements to traditional approaches for detection and response to cyberattacks [3]. Current approaches to cyber detection and response are based on static, reactive, often one-

This work is licensed under CC BY-NC-SA 4.0.

size-fits-all systems. In this scenario, only when an intrusion is detected, usually via an indicator of compromise detected by a proactive reactively mode, it will be needed to classify the type of attack/intrusion and assess the way it could respond. In addition to being ineffective in dealing with sophisticated or previously unseen attacks, this happens at the expense of excess trust and an important blind spot in the information concerning the security of the system prior to this point. AI, on the other hand, owing to its strong ability to learn and adapt, can offer a radically new strategy that improves the systems' security postures [9]. AI can be embedded within the security systems to offer a self-transformative adaptability of the systems' parameters.

One of the most powerful drivers of innovation and industrial competitiveness in the United States for the next half-century is technology advancement in networking, and digitization of manufacturing processes. The best implementation of this plan can be accomplished by leveraging the factory of the future vision with a focus on cybersecurity needs. Digitally connected factories provide opportunities for streamlining business processes, reducing costs, and speeding up time to market. The United States aerospace manufacturing (a niche of advanced manufacturing) industry supports national defense and critical infrastructure, while facing challenges such as protection against foreign navigation, expansion of global supply chains, and mandates to share sensitive information in networked environments.

5.2. Lessons Learned and Best Practices

This paper presents lessons learned and best practices through the creation and utilization of AI-enhanced cybersecurity solutions for protecting the U.S. aerospace manufacturing infrastructure. We believe that these technology development strategies, real-world deployment, and lessons learned will help guide researchers and practitioners in the field of computing, cybersecurity, and aerospace systems.

In modeling, one of the lessons learned is that emphasis must be placed on understanding the complexities. Though publicly available through libraries, the datasets still require a substantial amount of pre-processing to convert raw logs into sources and features needed for modeling. To better model the processes, additional data points are needed, but the limitations due to cybersecurity, business criticality of processes, or other constraints might

This work is licensed under CC BY-NC-SA 4.0.

prevent acquiring all necessary data. In terms of model performance, the requirements in cybersecurity are often more demanding compared to other domains.

In AI-driven advanced persistent threats (APT) and attacks, the statistically based detection models are utilized for security, thereby satisfying the nature of the attacks. The characteristic behavior of the average occurrence of individual cybersecurity CRT in the provided data is also more differentiable compared to the typical proportional differences found in data. Therefore, the performance metrics must take these constraints into account when evaluating the model and making decisions, and to optimize the chosen threshold of the coefficient.

6. Regulatory and Ethical Considerations

Regulatory and ethical considerations are critical factors in the integration of emerging technologies. Regulatory considerations regarding AI-enhanced cybersecurity measures in aerospace manufacturing include compliance with federal regulations, state regulations, industry regulations, and international regulations. Federal regulations that aerospace manufacturers need to comply with include the Cybersecurity Maturity Model Certification (CMMC) program, the Federal Information Security Management Act (FISMA), and the National Industrial Security Program Operating Manual (NISPOM). In addition to federal regulations, aerospace manufacturers must comply with state regulations, such as New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act. Other regulations that aerospace manufacturers may need to comply with include industry-specific regulations (e.g., ITAR and EAR regulations) [10]. Meanwhile, with AI-enhanced cybersecurity solutions being increasingly used in software products and services marketed outside the United States, aerospace manufacturers must ensure compliance with international regulations that restrict the export of certain technological capabilities (e.g., the General Data Protection Regulation).

The second layer of the risk management framework flags additional criminal policies and ethical considerations regarding emerging technologies. AI-enhanced cybersecurity solutions may raise ethical concerns regarding unfair bias, privacy violations, and the potential for a significant negative societal impact [11]. In particular, an imbalance in current capabilities between aerospace manufacturers and malicious actors may create an echo chamber that magnifies any negative societal impacts of AI-enhanced cybersecurity solutions. To address compliance and ethical issues relating to cybersecurity solutions in aerospace manufacturing,

This work is licensed under CC BY-NC-SA 4.0.

there are three recommendations. First, although all stakeholders recognize that aerospace manufacturers comply with multiple levels of federal regulations, they currently are not in place at the same cycle. Therefore, a systematic approach is needed to harmonize compliance cycles regarding federally mandated cybersecurity standards. Second, to monitor compliance with established cybersecurity benchmarks that consider COTS procurement, the creation of a program involving independent third-party certification would be an effective cybersecurity accountability mechanism. Lastly, beyond compliance and accountability, consideration should be given to social inferences regarding cybersecurity measures deployed in aerospace manufacturing.

6.1. Compliance Requirements in the Aerospace Industry

The aircraft manufacturing industry is one of the most robustly regulated industries. The entities that exist within this industry must comply with strict regulations from the Federal Aviation Administration (FAA) and the International Aerospace Quality Group (IAQG). This section elaborates on the regulations from these two agencies that cover the cybersecurity practices in place in aerospace manufacturing. It examines the guidelines under which the cybersecurity measures were developed in this project, as well as how the validity of the defense mechanisms is tested [12].

The industry that produces commercial aircraft and components places a high emphasis on their implications on public safety. Hence, the entities that cover this industry must comply with strict regulations from the FAA and the IAQG. The Federal Aviation Regulations (FARs) Title 14 Part 21 are a set of requirements that regulate the certificates of aircraft and airworthiness in the United States. The need to comply with the FARs as well as supplementary regulations from the FAA and the Department of Defense (DoD) depends on the certificate class of the entity.

The Quality Management Systems (QMS) standard AS/EN/SJAC 9110:2018 from the IAQG contains requirements for QMS in the aerospace industry. It is a supplement to the QMS standard ISO 9001:2015 and elaborates on stipulations in the FAAs' Advisory Circular (AC) 00-58B [8]. The AC presents minimum standards that a QMS must comply with in order for an entity to obtain a DoD or FAA certificate. A certification to AS/EN/SJAC 9110:2018 system without any deviations also guarantees compliance with the FAR Title 14 Part 21.

This work is licensed under CC BY-NC-SA 4.0.

6.2. Ethical Implications of AI in Cybersecurity

The implementation of AI-fueled cybersecurity approaches and remedies in aerospace manufacturing is not only replete with technological issues, but also with ethical challenges. Chief among these challenges are questions about whom decision-making authority over AI security systems ought to be entrusted to, how to guarantee proper use or non-misuse, how to ensure there are no unintended consequences and how to ensure the justification of a certain use of AI technology to be in compliance with relevant moral obligations [8]. These considerations regarding the ethics of AI-enhanced cybersecurity systems are bound to vary and interact with social and cultural beliefs and values, which in turn might influence one another. Some aerospace manufacturing firms may not be as concerned as others about the risks of detriment to personal freedoms posed by AI-naïve systems, while some rural communities' beliefs about the technological sophistication and safety of AI tools may differ from urban communities' beliefs [13]. General but unhelpful statements about ethics or fairness, or broad proclamations of robust tool capabilities, may give no assurance to worried publics about the social ramifications of current and emerging AI-enhanced cybersecurity systems. Discussions about in-depth analyses of the ethical issues mentioned above regarding the use of AI-enhanced cybersecurity systems as quasi-independent gatekeepers, advisors or overseers in aerospace manufacturing, will not focus only on questions about intended purposes or benefits. Analyses will also turn to the ethical principle under which the implementation of a certain AI-enhanced cybersecurity system in aerospace manufacturing or any other industry is deemed to have been faulty or inappropriate. Questions will include whether certain AI-enhanced cybersecurity systems might have unintended consequences, come to be misappropriated, or be subverted, or experience technical failures or loss of oversight. Whether some AI-enhanced cybersecurity systems' intended purposes or design features might hardly have been plausible if viewed through a lens of moral responsibility, or might even have amounted to happenstance or wishful thinking, will also be considered. Casting the net wider, it would be useful to examine the social, cultural or institutional conditions under which aerospace manufacturing firms would be culpable for the implementation of AI tools that came to violate ethical or legal obligations of fairness, non-discrimination or transparency.

7. Future Trends and Emerging Technologies

This work is licensed under CC BY-NC-SA 4.0.

This section examines future trends and emerging technologies in the realm of AI-enhanced cybersecurity for aerospace manufacturing. The world is witnessing the rapid emergence of new technologies that can change the way individuals live, interact, learn, and work. These technologies posses both benefits and threats. Cybersecurity for manufacturing is a concern, particularly in the aerospace sector where both incidents and regulations have an industry-wide impact. As a new wave of technologies emerges, cybersecurity is becoming paramount in protecting essential functions. The rise of the internet and the subsequent transition towards smart operations to fulfil the vision of 4IR have also opened pathways for cybercriminal exploits. AI-enhanced industrial cybersecurity solutions have flood the market to protect operations, and it is expected this trend will continue into the future.

Experts believe that current AI-based solutions are limited in overall effectiveness and that a new wave of AI-based technologies is needed. From next-generation AI to sensor technologies, the aerospace manufacturing industry must take note of the advancements to benefit from the available opportunities. This analysis examines outside traditional security measures in hopes of facilitating new technology advancement. The analysis concentrates on examining potential advancements that can disrupt the industry and shape its security landscape. It considers advancements relating to emerging capabilities associated with machine learning systems and impact across the range of hardware, software and procedural technologies.

7.1. Advancements in AI for Cybersecurity

Advancements in AI research, particularly machine learning (ML) methods, including deep learning, are expected to bring about paradigm shifts in several domains, including the cybersecurity domain of aerospace manufacturing [1]. At play here is a snowballing relation between cyber technology proliferation and an equal or greater response from malicious agents, both supported by deep investment in the research and development of offensive and defensive capabilities. In relation, recent advancements in the underlying cyber technology, such as the Internet of Things (IoT) and cloud computing, guarantee the continued dissemination of valuable assets across growing and increasingly complex networks. Coping with what may be an exponential growth rate in the number and sophistication of threats to these assets, however, is a considerable challenge for the aerospace industry. On the one hand,

This work is licensed under CC BY-NC-SA 4.0.

the inherent unpredictability of AI must also be tackled, which is monumental in terms of current understanding of basic questions such as what intelligence and thus AI really mean [3]. These advancements are rapidly penetrating the civilian domain, including aerospace manufacturing companies, and bring important challenges concerning their exploitation for malicious purposes as tools by hackers or as targets in impacts on safety-critical operations. On the other, dedicated efforts must be undertaken to assess the potential impact of AI on defensive capabilities and how to seize the opportunities presented by this technology disruption to rethink the future trajectory of cybersecurity practices in the aerospace manufacturing domain.

7.2. Impact of Quantum Computing on Cybersecurity

This growing threat warrants comprehensive investigation of many facets of AI-enhanced cybersecurity. Quantum computing, based on quantum physical principles (superposition, quantum entanglement, quantum interference, etc.) and a class of algorithms (e.g., Grover's and Shor's algorithms), is expected to exceed capability-wise the present-day (and next-generation) computers for a number of computationally hard problems and to transform the capability of cyber threats. In particular, while Shor's algorithm has the potential to break the widely used public key cryptographic schemes (currently widely used schemes to establish secure channels in the hybrid public key infrastructure, PKI), Grover's quantum algorithm has the potential to change the current best-practice half-to-full-length symmetric key cryptographic solutions to half-length solutions, which may require existing symmetric key infrastructures to utilize three times of the resources needed today.

Today's public key cryptography ensures secure communications between two parties exchanging messages over a non-secure channel, true or authenticating the integrity of messages transmitted by trusted personnel. When a public key infrastructure (PKI)-related cryptographic component is utilized to ensure secure communications, e.g., HTTPS, PGP, and S/MIME, public key operations are automatically embedded in communication protocols.

8. Conclusion

Recent developments in technology have significantly changed how entities design, develop and deploy aerospace components. The use of new technology to enhance manufacturing

This work is licensed under CC BY-NC-SA 4.0.

capabilities requires newly built designs that require individualized approaches with high specificity. Such designs have prominent risks as they require proprietary designs to be shared in new ecosystems involving multiple components manufacturers. Nation-state actors that can afford large intelligence budgets are incentivized and capable of targeting and stealing such sensitive information. The effects of recent events such as the COVID-19 pandemic and the Russian-Ukrainian conflict have exacerbated the situation as infrastructure companies feel supported to share sensitive manufacturing information with trusted partners abroad but are not fully aware of how to protect such information. One such sector is the US aerospace component manufacturing sector which has become the target of nation-state threats and requires informed balancing of risk/benefits of given digital approaches. Use of digital technology has allowed multiple companies to compose extended supply chains to speed up the design of complex and critical systems. Excessive sharing of sensitive information within such digital ecosystems has raised significant concerns related to supply chain security since companies can become vulnerable to cyber-attacks that target their peers within the shared ecosystem. Already in 2019, the US Department of Defense and other US defense industry stakeholders have been breached through supply chain cyber-attacks in which security vulnerabilities and insider knowledge have been retro-engineered and weaponized against the attacking entity. Such concerns have been particularly exacerbated in the US aerospace component manufacturing sector due to attacks by nation-state threat actors that follow a specific paradigm for stealing sensitive industrial information, i.e. attacks follow extensive reconnaissance where threat actors target firms that have inherited sensitive information gained by prior successful attacks.

8.1. Summary of Key Findings

Among the widespread consequences of the global COVID-19 pandemic and the concurrent geo-political instabilities, recent cyberattacks against major U.S. aerospace manufacturing companies shine a spotlight on the emerging and escalating cybersecurity risks of supply chain infrastructures. These events have also fueled discussions on critically important national testing and validation infrastructures for aviation safety assurance that are uniquely provided by U.S. aerospace manufacturers, and the potential impacts that unintended access or disclosure of these infrastructures may have on aviation safety as well as on the design of U.S. fighter and commercial aircraft [1]. The combination of these recent events with the

This work is licensed under CC BY-NC-SA 4.0.

discussion calls for urgent cybersecurity review and enhancements and thus presents a unique opportunity to devise innovative cyber-attack detection and prevention designs using advanced technologies. Addressing cybersecurity issues has always been a U.S. priority in keeping national infrastructure safe, but more needs to be done.

Emerging technologies such as networking, data-driven artificial intelligence (AI) and machine learning (ML), 5G wireless, and the industrial internet of things (IIoT) create enormous opportunities for agility and efficiency improvements in aerospace manufacturing. However, cybersecurity must be equally advanced so aircraft and/or weapon specifications, trusted design and manufacturing processes, and sensitive supply chain information are not irretrievably compromised [2]. This theme provides an overview of recent concerns and challenges, as well as an introduction to relatively recent advancements in AI and ML that inherently exhibit multiple learning and processing perspectives. By taking a comprehensive view of the problem, including knowledge uniformity, ambiguity, and vagueness, a path towards cybersecurity enhancement is facilitated. In consideration of emerging aircraft, weapon systems, and aircraft architecture, this theme seeks to stimulate discussion on immediate challenges for fully autonomous aircraft systems, such as recent industry accusations involving unfettered access to adjacent controlled manufacturing systems as well as misinformation and denial-of-service cyberattacks on autonomous systems. Recent events involving a missile being unintentionally launched as a consequence of a design error unveil the challenge of blindly trusting AI as a human fallback.

8.2. Implications for the Future

Many factors will influence the outcome of the severe challenges faced by the U.S. aerospace manufacturing sector as a result of deep, destructive, AI-enabled cyberattacks on the nation's manufacturing infrastructure. A few of the factors likely to play central roles in determining the outcome of this situation are as follows.

Will a suitable AI-enhanced cybersystem cybersecurity solution to thwart deep cyberattack/enhance overall cybersystem security, resilience, and efficacy/efficiency be developed and deployed in time? This AI-enhanced cybersystem cybersecurity solution would need to be purposeful in its offensive/defensive capabilities as well as in its design (i.e., for ease of deployment). It would also need to be coupled with an entire continuum of

This work is licensed under CC BY-NC-SA 4.0.

societal/political/educational/industrial/cultural considerations and possible deep transformations thereof (e.g., in education, large parts of societal culture, including deep-seated images of privacy and trade secrets/market competitiveness which might need to be transformed, etc) in order to be implemented and actually deployed. Then there is the question of how to convince people to act; this would vary from nation to nation [16]. The collective vs individual images, use of fear, etc., are just a few examples of the nuances that would need to be carefully managed. A necessary first step in the transformation of these societal concerns/images into something actionable in a cooperative, timely manner may need to be addressed urgently and thought through carefully. This could be part of a broader approach to deeply rethink, collectively, how societies on Earth and the solar system should be coevolving with increasing intelligence across different forms of intelligent entities/minds. Currently, it seems as though this concern, particularly for slowing down the race as well as addressing it as a deeper societal transformation is not necessarily in the forefront of nations' awareness and attention.

There are also many unknowns in this space as to how deep a downfall scenarios and consequences would entail. There are deep uncertainties associated with almost every dimension of the above factors, including the causal relationship(s) which would play out amongst this web of interactions would unfold. The possibilities span a wide spectrum of possible futures for humanity and life on Earth.

Reference:

1. S. Kumari, "AI-Enhanced Agile Development for Digital Product Management: Leveraging Data-Driven Insights for Iterative Improvement and Market Adaptation", Adv. in Deep Learning Techniques, vol. 2, no. 1, pp. 49–68, Mar. 2022
2. Tamanampudi, Venkata Mohit. "A Data-Driven Approach to Incident Management: Enhancing DevOps Operations with Machine Learning-Based Root Cause Analysis." Distributed Learning and Broad Applications in Scientific Research 6 (2020): 419-466.

This work is licensed under CC BY-NC-SA 4.0.

3. Machireddy, Jeshwanth Reddy. "Assessing the Impact of Medicare Broker Commissions on Enrollment Trends and Consumer Costs: A Data-Driven Analysis." Journal of AI in Healthcare and Medicine 2.1 (2022): 501-518.

4. Tamanampudi, Venkata Mohit. "AI-Powered Continuous Deployment: Leveraging Machine Learning for Predictive Monitoring and Anomaly Detection in DevOps Environments." Hong Kong Journal of AI and Medicine 2.1 (2022): 37-77.

5. Singh, Jaswinder. "Social Data Engineering: Leveraging User-Generated Content for Advanced Decision-Making and Predictive Analytics in Business and Public Policy." Distributed Learning and Broad Applications in Scientific Research 6 (2020): 392-418.

6. Tamanampudi, Venkata Mohit. "AI and NLP in Serverless DevOps: Enhancing Scalability and Performance through Intelligent Automation and Real-Time Insights." Journal of AI-Assisted Scientific Discovery 3.1 (2023): 625-665.

This work is licensed under CC BY-NC-SA 4.0.