Fabrication Process Integrity Monitoring and Insider Threat Detection: AI-Enhanced Cybersecurity for U.S. Semiconductor Manufacturing Infrastructure

Dr. Henrique Sentieiro, Professor of Informatics, University of Coimbra (UC)

1. Introduction, Developing effective techniques and systems to protect the United States semiconductor manufacturing infrastructure is more critical than ever, given the looming strategic challenges to their supply chain resiliency. AI-enhanced cybersecurity is a particularly promising solution to the current strategic supply chain security crisis. To that end, this report (1) discusses a model of strategic supply chain security to clarify the sources of risk and the nature of possible solutions, and (2) introduces the set of papers here to explore AI-enhanced cybersecurity by entities seeking to protect their own supply chain interests, and (3) innovators and policymakers seeking to provide dominant solutions for attackers, terrorists, and potential future adversaries. The essays draw on a conference that brought the cybersecurity industry and the federal government together, and we are grateful to both the speakers and the attendees who motivated, encouraged, and improved our work.

U.S. microelectronics are critical to the national and economic security of the United States. And yet, the meltdown of the system's global supply chain caucus, especially in the face of the ongoing semiconductor shortage, indicates that foreign semiconductor manufacturing has put the United States in a vulnerable position. The situation becoming more rather than less difficult is further stimulated by executed and announced actions among the big three firms: Taiwan Semiconductor Manufacturing Corporation's (TSMC's) willingness to build a plant in Arizona is more of a lease agreement, according to many experts, and the only new U.S. Intel fab (Technology Development) is forecast to be down due to close next year. Moreover, the other two U.S. leaders are relying on contracts for semiconductor chips fabricated by independent foundries (Intel) and TSMC (Apple). Adversaries are thus pursuing multiple lines of attack when it comes to adding, slowing, or ultimately restricting the ability of U.S. manufacturing firms to produce semiconductor chips. Finally, PE's recent strong rating of potential impacts on U.S. manufacturers made possible the business impact of these attacks.

1.1. Background and Significance

Sensors and built-in self-tests have become critical for successfully scaling beyond the 5-nanometer node. As such, U.S. semiconductor manufacturing is faced with vulnerable technology that offers adversaries opportunities to access sophisticated hidden backdoors. Enhanced cybersecurity solutions will aid our nation against cyberwars ranging from mere information collection to physical destruction of our power infrastructure. For example, a compromised IoT device could launch a distributed denial-of-service attack on one of the many components of the control/data acquisition system used in a U.S. semiconductor wafer fab. Even relatively small cyber disruptions could cost a U.S. semiconductor wafer fab millions in downtime.

Furthermore, although the overwhelming majority of semiconductor designs and applications behind U.S. companies' TMSA were never manufactured in China, or on Chinese equipment or tools, the same power IC design and application processor designs can be manufactured and duplicated in China without the design owner's consent. As a result, the same U.S. company's power ICs shipped abroad could power weapons systems openly sold in foreign electronics markets. Similarly, a Chinese factory reverse engineering deployed chips in such weapons could over inscribe them with embedded backdoors capable of wreaking ferocious AI-powered havoc on U.S. systems. There's a critical chink in U.S. semiconductors, and we ignore it at our risk. It is time to begin anew the arduous process of "reshoring" some semiconductor manufacturing for the security of our nation. Furthermore, it is critical for trusted foundries overseas to adopt the AI cybersecurity technologies that are researched and delivered in this whitepaper. Failure to do so would open the world to unacceptable physical and economic threats. The collection of AI cybersecurity tools that have been demonstrated on a comprehensive number of test-chips, wafers, and other test vehicles by SkyWater Technology Incorporated, University of Florida, and i3 Electronics, offer a precompetitive solution applicable to every chip and manufacturing flow, simple to apply, that have low operational costs per wafer. We present all these results in this whitepaper.

1.2. Research Objectives and Scope

The primary goal of our study is to be a single source of information on the complex topic of cybersecurity in the semiconductor industry and to place the U.S. geography

into the context of this topic. By conducting this research study, we aim to explore the role of AI in enhancing cybersecurity solutions, as emerging industries like freestanding IC manufacturing, for instance, might employ AI to begin with security in mind. The artificial intelligence techniques of solutions available in today's market for the U.S.'s semiconductor infrastructure have either been directly explored in the context of individual fab operations or have been used more broadly for enhanced IT/OT security solutions. Besides providing an overview of the main principles and techniques behind AI-enhanced cybersecurity solutions, we also aim to evaluate any instances where such a technique has already been employed in the real world. Finally, we will conclude this study by suggesting a roadmap, explaining in more detail how our goals should be achieved. There are multiple segments, each with its own set of goals, that together enable the completion of the above objective.

First, by observing principles and instruments of existing security technologies, we will address the inter-industry, supranational, and scientific relevance of the use of AI systems in protecting a state-of-the-art, U.S.-located semiconductor manufacturing infrastructure. Secondly, we explore the scientific principles, concepts, and terminology that allow AI systems to be adapted. We will proceed to present these as solutions. More importantly, we will describe the systems that underpin and enhance the local security policy frameworks. In the third place, we are going to study the evolution of industrial IoT, known as Industry 4.0, which will show that we must include unique cybersecurity security by design techniques, from the ground up, in such architectures. We will be discussing how the IoT and ICS subnet incorporating any aspects of the 4.0 building block need to be built. We will give an assessment of the natural upgrade to a protection scheme that works together in our last segment. The key is to develop a connection that connects the ICS and the IoT so all subsets must be protected to achieve the highest national security standard.

2. Cybersecurity Threats to Semiconductor Manufacturing

The cybersecurity threat landscape affects every aspect of modern society. This report focuses on the domain of semiconductor manufacturing, which is essential for the modern U.S. economy. The manufacture of semiconductors is capital- and knowledge-intensive and involves numerous interconnected stages requiring many kinds of high-tech equipment. In particular, the fabrication process, called wafer fabrication, is an

important part of the overall manufacturing. If an attacker can disrupt this process without drawing immediate attention, then components containing unknown vulnerabilities may enter wider circulation. Eventually, an unaware victim may suffer loss as cheaper subverted components fail or are manipulated.

The control systems present in semiconductor fabs present an attractive target for nation-state adversaries and other actors. Semiconductors are perpetually a high-value asset. While small in size and light enough to be smuggled into targeted spaces, secrecy of semiconductor manufacturing can lead to very offline yet very effective operations. Given that semiconductor manufacturing is primarily conducted in multiple facilities across a handful of defender-controlled territories, it is much easier to watch them directly than critical infrastructure which is landlocked through adversarial territory. Thus, it's much easier to ensure sufficient internet-free locations exist to drop compromised elements. To begin with, a threat actor involved with fabricating or assembling semiconductors may take advantage of their access to plants and knowledge about processes to subvert the operation of the equipment. The techniques commonly employed by the Big Nine are a form of these threats, although a highly targeted form. There are three specific cybersecurity threats that could be faced as sub-themes.

2.1. Overview of Cybersecurity Threat Landscape

Today, state and non-state adversaries have become increasingly advanced and more willing to engage in disruptive activities. As the Cybersecurity and Infrastructure Security Agency (CISA) observed, the range and level of sophistication of threats continues to grow at an alarming rate, posing increasingly critical challenges to organizations across industries. Sophisticated ransomware and state-sponsored attacks (such as the ones targeting largely unpatched software supply chain in 2021), deep fakes, cross-domain distributed denial-of-service (DDoS) attacks—DDoS attacks that ramify from a state or enterprise network into the broader Internet—are only some examples of rapidly evolving threats. They will inevitably require more creative and collaborative approaches to address than traditional IT or operational technology (OT) security solutions can offer. However, most organizations, including those in the semiconductor manufacturing industry, not only lack the necessary AI expertise but data too in order to devise such advanced security solutions.

Many threats persist and evolve due, in large part, to the legacy systems still used across industries. More secure, yet cost-competitive hardware and technology largely do not exist for semiconductor companies to be able to update their threat models, resulting in a significant impact on the security postures and growth of the United States. Investment in AI-enhanced cybersecurity solutions, including advanced microelectronics and supply chain security vetting, to protect United States semiconductor manufacturing infrastructure not only is essential for businesses but is a critical national priority.

2.2. Specific Threats to Semiconductor Manufacturing

It is these targeted threats that are particularly relevant to semiconductor manufacturing. The cyber threats posed to semiconductor manufacturing are both varied in their taxonomies and numerous, from the simple attacks due to a lack of basic cybersecurity hygiene to highly sophisticated, nation-state sponsored espionage events, which themselves vary by tactics, techniques and procedures (TTP). Note these examples are all referenced in the MITRE ATT&CK for Cyber Replication as some of the provided resources. The sight of successful, if only temporary, compromise of our prime and above design firms like Intel, AMD, TSMC and others further show these threats are not only real, they happen regularly. As a result, protecting semiconductor manufacturing from cyber risk cannot simply pivot around a perfectly functioning preventative or predictive security model.

A significant section of commonly recognized cybersecurity threats is based around nation state espionage, industrial sabotage and/or the ability to degrade supply chains. In security parlance, this requires a level of APT/DIB/SNAZTI attacks. Most of these attacks leverage bespoke malware driven by human actors in order to bypass normal corporate security. These exploitation processes often involve a wide variety of cyber attack vectors. In combination with the characteristics inherent within most semiconductor supply chain manufacturing, these attacks are also potent. Due to geographical dispersion, the predominantly ICT-based engineering, the concepts of global partnerships and the automation and data sharing features of Industry 4.0, what is identified as the industry is generally spread across the globe in a linear sequence of factories and offices known as fabs.

3. Fundamentals of AI in Cybersecurity

3.1 What is AI? Artificial intelligence (AI) is a branch of computer science that develops intelligent machines, applications that can perform tasks that would typically require human intelligence, such as learning, comprehension, problem-solving, and decision-making. AI leverages pre-existing algorithms to mimic human intelligence and to help systems adapt and evolve. Machine learning (ML) is generally considered as a subset of AI and can be divided into supervised, unsupervised, semi-supervised, and reinforcement learning.

3.2 Relevance of ML and DL in Cybersecurity This section covers some basic concepts that are often associated with machine learning and deep learning technologies that are most likely being utilized to enhance multiple cybersecurity areas associated with risk mitigation and threat detection but not exclusively. Since they cover the fundamentals of the AI that are being utilized in CISMIC, they serve to provide a context for other readers less familiar with these techniques.

3.3 AI Technologies in Cybersecurity Microsoft studied AI threats that attempted to break into Office 365 environments. On a global scale, compared to other industries, semiconductor manufacturing saw a higher-than-average number of phishing threats coming from malicious websites. Phishing threats are those that may prompt users to enter credentials. Phishers often use this information to access and infiltrate accounts and are the most common threat in the study. In this report, AI can be used to create a more secure environment in the office governing phishing and malware campaigns are going to be the subject of study. These conclusions will tell a clear story demonstrating the effect these attacks are having on businesses everywhere. They will also explain why having an AI solution in place can help avoid a potentially costly breach or a comprehensive action. AI has a plethora of applications within the field of cybersecurity.

3.1. Machine Learning and Deep Learning Basics

In more than one decade, the machine learning approach has been the main factor in cybersecurity. Machine learning is a subfield of artificial intelligence (AI) that provides systems the ability to learn and improve from experience. In fact, a more concrete description of machine learning is provided by Suresh et al. in their book, which describes machine learning to be a form of data analysis that automates analytical model building. This (machine learning) is not only the process that provides analytical model

building, but it is also a process by which model building begins, and the system itself identifies patterns from the processed data (observations) that are not explicitly programmed.

Deep learning is not different from machine learning besides providing the basis of the level of learning models being built. Deep learning itself is machine learning that runs at high level abstraction, which is to understand data in terms of hierarchy. Deep learning does this through the data in the neural network model (artificial) that simulates the structure of the human brain. The neural network architecture begins with a simple problem or concept, and as the data increases, the neural network architecture finds somewhat complex concepts. AI in the form of deep learning is indeed popular mainly among experts or geeks, but that does not mean its use is so practical and easy to use. The deep learning architecture is related to neural networks that are complex and consume time and resources, as well as the expertise and computing capacity that are quite different from ordinary ML.

3.2. Applications of AI in Cybersecurity

AI technology has become a game-changing factor in the field of cybersecurity. Automated systems driven by AI technologies have the potential to zero in on security threats, predict and prevent security breaches, help businesses manage their security tools, and become more secure over time. Given the speed of advanced cyber attacks, AI is unmatched in its response time and can automate reactive solutions in a fraction of the time it would take for a human to react. AI also thrives at mitigating existing and future threats because its "smarts" run off historical data capability, i.e., it continuously "learns" from the data it processes and becomes progressively better at identifying out-of-the-ordinary activities that could signal a security threat. AI technologies are now being used in numerous segments to develop various tools and mechanisms to protect assets in cloud, mobile, computer systems, ICS, and SCADA.

The application of AI in several areas, such as remote data analysis, identity verification, fraud detection, speech recognition, face detection, language and data processing, as well as spam filtering and anti-malware in emails, is already existing AI technologies to improve the security of computer systems. Various segments and applications where AI is currently being used are listed here as follows: AI technology with temporal, ICS with spatial, network with cascades and emerging networks, information and system security

testing with verifiable and demonstrable, wireless and mobile security, and specific to critical infrastructure protection. AI technologies such as neural networks, expert systems, machine learning, etc., have been utilized to detect intrusions in computer systems by monitoring users' activity, controlling changes of OS, threshold, etc., and to predict the incorrect usage of programs running in the cloud and smartphones.

4. AI-Enhanced Cybersecurity Techniques

Information Loss Prevention (ILP): Thousands of elements are dangling in a large-scale network and hold certain information, including personal information, credentials, and valuable knowledge. In the utility case, we can differentiate two network elements according to their knowledge relevance. For example, in telecommunications, we have elements that do not possess any personal information while others know your location or that you have a particular illness information. This will be even more relevant for 5G when all kinds of devices that hold personal information will be connected to the network. At any given moment, the task of the AI is to find out which knowledge-pertaining elements can potentially interact, both directly and transitively. Once the adequate subsets of AI-knowledge-dangling elements forming a big graph are unioned and therefore located, all these AI-adjacent elements from all the graphs can be isolated from their adjacent group on previously non-exposed AI-irrelevant set of network elements.

In a cyber-attack scenario, ILP techniques can specify what confidential information was gathered, conceivably decrypted, and exfiltrated. Hence, we identify a list of elements susceptible to reaching the suspected vulnerable network elements to produce a network report. This, in turn, will limit and control the distributed knowledge needed to conduct a social engineering attack to a reasonable minimum. Together with Native AI, we can pursue the mining task of finding the knowledge connection between the victim and other potential members of a collusion attack. In the above, AI can inform subject matter experts of the list of particular, highly knowledgeable, network members that can be most useful and important to an adversary.

4.1. Anomaly Detection

Anomaly detection is a technique to be used in the efforts to protect these systems from impending attacks. It has been widely employed by developers for various applications in terms of practical challenges. In semiconductor manufacturing sectors, there is a

significant demand for detecting unanticipated danger in these environments. These data streams are usually multivariate and segregated in nature. Due to this reason, these databases might have irregular patterns. Our proposed algorithm employs data from up-to-date sensors measuring the semantics of the environment signals and hence the data volume is huge. The main focus is to thoroughly investigate a method for each sub-problem that is both viable and reliable, as well as to address real-world problems. Our anomaly detection procedure can be employed in the semiconductor manufacturing environment.

Despite having a process to monitor the observations from the data stream, one cannot eliminate the raw data from the database. We perform an analytic search of the data stream in order to detect unusual behavior in the databases. Considerable quantities of data flow from the enormous number of sensors linked to the database in the semiconductor manufacturing systems. The trend displays some anxiety as to what an unexpected shift in the database can carry out in contrast to the evolution of data flow in the event of the planned change of the shift. We are in need of an efficient method to identify the novelty in the databases when they display an irregular outlier from the data flow. The suggested method is productive, plays well with a high level of accuracy, and has the potential to detect an unusual shift in the industrial environment.

4.2. Behavioral Analytics

Behavioral analytics, also known as user and entity behavior analytics (UEBA), is a cybersecurity prevention and detection technique that leverages the power of AI to identify threats to IT infrastructure and security systems by recognizing patterns of behavior and identifying anomalies. Under the semantic approach, an anomaly is understood as a deviation from the statistically or previously traced patterns and different from a semiotic approach that may also consider knowledge gaps or even the ability of constantly learning about. UEBA types of AI-enhanced solutions are related to target discovery and attack detection efforts and can provide the user with fully automated or semi-automatic continuous process of detection, classification, and prioritization of potentially critical security risk situations, covering threats originating within and outside the U.S. and compromising the Intel developed and acquired equipment and proprietary cybersecurity solutions used in our evaluation projects. For instance, the AI-enhanced behavioral analytics technologies that themselves fall among

the topmost secured systems, i.e., those without the authentication management aspect, currently have commercial applications within the European Union for detecting both data leaks and cyber-physical system malware attacks in industrial automation-based Industry 4.0 deployments. This makes such AI-enhanced technologies closely relevant for enhancing the capabilities of resilience in the U.S. semiconductor manufacturing sector, especially when extended to authentication-based access.

Recent Real World Behavioral Analytics As per "by 2023, over half of companies consider the accuracy enhancement of high-precious business-critical decisions continuously with AI under cost and significantly also a business requirement". Using AI for ensuring fraud detection and monitoring is among the top ten banking and financial services automation projects that are expected to play the critical role leading up to and including 2025. IBM Security and Ponemon Institute reported that the number of the AI and ML platform users is gradually rising in response to the rapidly-evolving threat landscape. Irrespective of the complexity and sophistication of the cyber-attacks, almost 60% of completed AI automation users expressed high confidence in their ability to differentiate the risk-based threats from other intrusions and loss of data. Security-automation freshmen (the non-users and prospective) have also demonstrated a growing interest in using AI as an alternative to training the human cyber-analysts and largely gaining visibility with respect to their enterprise-wide hacking and reconnaissance activities. In a related development, Cyber published a unique, patented "cyber behavioral & profile-analytic built from AI and ML" model in Mar, 2022 using one-touch-cyberthreat-profiling in as little as 5 min instead of days for defending the top U.S. utility companies. With the continual increase, AI-based platforms for cybersecurity are being used to quickly and accurately model updates and old-threat threat divergence adapted to changing behavior. AI-enhancement powered, dark analytics supply chain technologies for industry, the business, and government are on the quick-rise and have already graduated or have been selected for U.S. DoD Commercial Services Accelerator.

4.3. Threat Intelligence Integration

An important part of the AI-augmented cybersecurity data collection process consists of enriching and augmenting diverse sources of data with qualitative and semantically meaningful metrics. One of the most effective and widely applied AI-enhanced

cybersecurity techniques is threat intelligence integration. Threat intelligence consists of knowledge about adversaries and threats, which can be used by organizations to make more informed decisions pertaining to their defenses. The main strength of threat intelligence is that the collection ranges from the most active attackers to conducted research resulting in the make-up of several large companies specializing in selling threat intelligence reports. Organizations and companies working on research into cybersecurity attacks share the data obtained during such research because this is widely informally accepted as a negative externality for the attack surfaces of publicly released targeted entities.

Threat intelligence can only serve one purpose—to support better decision-making. Because of this, placing threat intelligence at the service of organizations' defenses means amplifying their effectiveness. Consequently, integrating threat intelligence into the multiple defense systems of an organization means repurposing or enforcing those defense systems by leveraging the knowledge and insights from many diverse sources. Defenses that are augmented with this knowledge are naturally expected to defend more, and do so more effectively compared to those who do not. Essentially, taking advantage of publicly available knowledge allows an organization to supercharge their defense systems with expert aid from the outside in real-time. Integrating threat intelligence data is, as such, a vital and essential component of AI-augmented cybersecurity.

5. Real-World Applications in Semiconductor Manufacturing

In this section, we discuss real-world applications that use AI-enhanced cybersecurity solutions developed by the companies who submitted the original response to the RFI. In each of the subsections, we discuss a brief overview of the technologies proposed, how they can be used in the real world, and include the companies' individual case studies that demonstrate a successful application within the semiconductor manufacturing sector.

Case Study: A Large Fabless Semiconductor & Microcontroller Manufacturing Business Unit Overview:

Large Company: 100K+ Employees, Publicly-Traded, $$$B+ In Revenue

Business: 2000+ Semiconductor IPs, Fabless & Silicon Foundry

AI Cybersecurity Solutions Developed: Automated Anomaly Detection, Continuous Cyber Risk Monitoring, and Cyber Vulnerability Mining

Overview: The technology from the company can detect abnormal "non-cooperative" or "malicious" behaviors of computer systems that other cybersecurity solutions (cybersecurity experts, purpose-built solutions, or specially trained AI) cannot. The technology can recognize software, systems, infrastructure, hardware, and networks that are working "as expected" and are "good." It can identify threatened or "compromised" assets that are operating at risk for today's risky environment. Further, AI is qualified to identify which non-normal behaviors found cyber weaknesses or vulnerabilities (IT as well as OT) that need to be addressed. We use aggressive predictive alerts with far fewer false-positive and false-negative alerts than any competing technology.

AI can adapt to rapidly identify newly identified cyber weaknesses/vulnerabilities revealed in everyday functions such as a cyber attack or problems with a new software/hardware upgrade. The company's specific applications enable businesses to: Gain end-to-end insight into ongoing and potential cyber vulnerabilities in operational as well as business IT and security domains. Cybersecurity risk is determined by profiling cyber behaviors, linking intense measures in securing critical equities, and identifying helpful methods for reducing cybersecurity costs. The platform unites IT and OT security enabling focused risk management and immediate expert technical help via patented real-time understanding and rapid active remediation.

5.1. Case Studies and Success Stories

The lack of use cases and success stories in recent literature suggests significant challenges in producing beneficial solutions for the deployed applications. Whether it is due to proprietary and context-sensitive results, strict intellectual property protection policies, or the complexity of real-world applications, these factors make it difficult to assess success and risk trade-offs without the provision of evidence showing the achievements of the proposed solutions.

In this section, we present two use cases developed by IBM and KPMG expert teams where they reviewed a real-world application of AI-enhanced cybersecurity for U.S. semiconductor manufacturing. Real challenges, threats, assets, and trade-offs of the two deployments are discussed. The case studies are used as guidance tools to shed light on

practical research, focusing on the requirements, threats, opportunities, effectiveness, risks, and interaction with other enterprise processes likely to be encountered in real applications. The deployment of the successful use cases underscores the prospects for AI-enhanced cybersecurity in real-world adversaries' hands when applied to the protection of U.S. semiconductor manufacturing.

In this section, we present two applications of AI-enhanced cybersecurity for U.S. semiconductor manufacturing. Our goal is to inform cybersecurity researchers about the challenges, risks, and practical success of such applied research by delivering the details of successful real-world applications. Both of the use cases provided are based on real practical examples currently in development, and we describe how they were developed in the sections below. Each deployment includes DL approaches and solution architectures. Finally, relevant enterprise cybersecurity requirements and how the technical solutions support the requirements are detailed, either directly or through impact. The first use case is a privately developed validation framework designed to defeat security breaches at chip manufacturing plants. The second use case involves a proprietary app designed to keep malware from propagating across any installed chip globally.

5.2. Challenges and Limitations

Despite the wide application of AI in the field of cybersecurity, implementing AI-enhanced cybersecurity techniques may not be a feasible choice for semiconductor fabs for many pragmatic reasons. The core of the matter is that individual cybersecurity protection techniques available in producing pipelines are established on diverse rules and regulations at the different layers of the pipeline. These principles were developed according to the company's necessities, which include the reminiscence of the company's uncommon topological configuration and semiconductor-related operations.

Cyber vulnerabilities are distinct at each SEMIFAB due to the continuous development of semiconductor technology. As a result, the chance of breach due to an unobserved vulnerability can be the highest when AI-enhanced cybersecurity techniques are implemented in the perspective of utilizing a pre-established model. Another important couple of challenges that must be noted are associated with the development and validation stages of these AI-enhanced cybersecurity techniques. The development of these techniques will require expertise in both the domain of cybersecurity and AI.

Moreover, it may be expensive for many companies to find both experts having expertise in both domains or hire two experts. The validation of these systems adds an extra layer of complexity. Since many cybersecurity protections are in place already, it is difficult to access a live cybersecurity incident. Consequently, a technique to validate AI-enhanced cybersecurity will need extra considerations. With all these potential issues, in the real world, engineering expertise with AI continues to be in a very baby stage, which subsequently may not permit good growth in that course.

6. Regulatory and Ethical Considerations

An overarching framework for evaluating the ethical issues of augmented cybersecurity is the regulatory landscape designed to ensure assurance in both AI-enhanced systems as well as user privacy, from multiple perspectives. Regulatory compliance in sectors that increasingly rely on AI is becoming essential for purveyors of secure and responsible technology. Thus, identifying possible applications and requirements as they may affect semiconductor manufacturing is a principal consideration for inclusion in this chapter.

Certainly, one of the most significant challenges to fielding any AI within the cybersecurity landscape, and may be counted as a de-facto requirement, is the potential collection, storage, and use of personally identifiable information (PII), which may be further categorized based on location to be either of European Economic Area (EEA) or United States person (US-PII). At a minimum, any analysis of workforce data will implicitly involve location-specific information. Further, where relevant applications (for instance, using cameras and sensors to track activity by humans) must comply with privacy laws, these solutions will have additional legal, security, and ethical challenges. Where commercially available solutions may be employed, these considerations form a significant slice of the impetus when selecting which cybersecurity applications present a best-fit solution.

Nothing in this chapter should be construed as advocating or proscribing a specific course of action. Rather, the goal is to evaluate both a variety of challenges which may be encountered in implementation, and various compliance issues which must be weighed as potentially large "cost multipliers" for legal, regulatory, and ethical reasons. To address these varied concerns, access control, secure authentication, privacy-

enhancing technologies, and data minimization might be used to architect for adherence to the principles that underlie both cybersecurity and data protection.

6.1. Compliance Frameworks

For effective integration of the proposed system detailed here, it is important not only to follow but to also demonstrate how our methods improve established standards, containment procedures, and IoT security guidelines for protecting manufacturing facilities, regime tools used in safeguarding semiconductor production, emphasize the utilization of regulations set forth by the U.S. Office of the Press Secretary for national policy, DD-21 for defense acquisition for manufacturing, and defense procurement of the Commercial-Off-the-Shelf (COTS) hardware. The AI enhancement on its own is not enough to gain support, and without a showing of compliance and smart integration into the policy and real arena, argument for its use does not hold. For these reasons, clear, easy explanations of AI decision making will go beyond the need for the system to learn on-the-fly and possibly harm operation to potentially becoming a standard to promote best practices within asset protection regulations. It must be easy to demonstrate to "unlock widespread interest in further use", and the Ames Lab will work with policy organizations toward making that happen if this paper is further funded.

Research from the lab suggests that if two of five different sensors malfunction at the same time due, for example, to a cyber attack from within the system, it would likely impact the plant's operation. The sensors are vital and so much equipment is connected to them in a manufacturing operation like this. Regulatory agencies consider failure of such equipment during a natural disaster, such as earthquakes and floods also. Further, one must provide a commercial pathway for widespread manufacturing of this equipment, not just in U.S. Microelectronics Hub, but in Asia, Europe, and South America. Any new technology deployed must be careful not to add additional points of failure and must follow the applicable international standards for performance, robustness, and durability. In reaching our system above, we can reference the following National Programs as the basis for each facet described in what follows: National Advanced Packaging Manufacturing Resource Program whose discussion should include the U.S. National Policy and Other National Programs with which a solution, such as the one proposed for operation in collaboration with the lab, must comply.

6.2. Privacy and Data Protection

Privacy and data protection. It is essential to consider privacy and data protection issues when designing and deploying AI-enhanced solutions for cybersecurity inside a semiconductor manufacturing environment. Given that many of the AI-enhanced technologies described herein use video, audio, machine log, network packet, or employee transactions and access data feeds for cybersecurity, it is essential to collect and process personal data in accordance with privacy and data protection regulations and ethical practices. Semiconductor manufacturers have an ethical responsibility to protect the privacy and data rights of their employees as well as other third parties who work within their facilities and campuses. Given that not all techniques rely on external data collected by AI-embedded sensors, some are entirely non-invasive and solely leverage digital feeds and access logs specifically exempt from most privacy regulations and ethical considerations.

Video cameras and microphones are also essential safety features in many operating environments to protect employees from various risks, including collision and personal injury, explosion and fire, chemical exposure, and to avoid hazardous materials, including inert gases that can displace the oxygen required for life outside sealed facilities and wafer fabs. In addition to safeguarding privacy and data protection, it is also essential to ensure that the use of AI-enhanced solutions for cybersecurity follows all relevant laws, rules, and regulations. In Europe, the General Data Protection Regulation (GDPR) sets a general standard for data and privacy principles and a focus on the rights and freedoms of individuals and applies across the European Economic Area. In the United States, the National Institute of Standards and Technology (NIST) and Federal Trade Commission (FTC) published guidance on the intersection of AI and law concerning the protection of personally identifiable information (PII). In many cases, other legal frameworks may apply to the use of AI-enhanced cybersecurity solutions. These legal and regulatory requirements must be addressed when developing and deploying such technologies.

7. Future Trends and Directions

AI in cybersecurity will keep evolving. In the next few years, the researchers, developers, and practitioners will invest a lot of effort to go beyond detection and focus on related cybersecurity aspects. The significant strides to move towards this direction

will create the threat hunting domain. Threat hunting is the proactive approach that can deal with attacks with no indicators of compromise in the system. These changes will allow the research community to use AI for cybersecurity problems in a more sophisticated and advanced manner. The research in AI-related technologies and their real-world applications will evolve according to these future trends as well. We anticipate that AI-based security solutions can be used to protect the US semiconductor manufacturing infrastructure.

The combination of spectrum sensing technologies with the intelligent detection and AI algorithms embedded in the wireless networks to perform spectrum security enforcement has taken a large research step towards practicality. The introduction of such technology could have applications in sensitive commercial critical infrastructure areas, e.g., manufacturing (Intel FAB), where investment in spectrum sensing or infusion into current network infrastructure for security are very real prospects. In these environments, interference is not permissible, but it is hard to enforce network device security at the periphery (sans-complex, expensive screening THz X-ray static scanners). If secured, containing quantum dots that react to spectrum probing to actively mitigate probing location through transient channel drift could enhance the utility of intelligent spectrum security. As a nation, the great interest in moving semiconductor manufacturing back to the US increases the value of protecting such manufacturing facilities. While such a narrow AI application might seem like a very niche area (though it has commercial ramifications), the goal is to present a wider appreciation of AI and security protections potentially available. We find the use of MANOVA to optimize for coverage parameters to be both a unique and novel application, and of broad interest to the community and the security. Such security represents the type of technology that is cutting edge, is of national interest, and represents economic investment in US infrastructure.

7.1. Advancements in AI for Cybersecurity

Over the last two decades, AI has developed into a field of great excitement and promise, especially in the area of cybersecurity. As of 2021, the approach that has been most consistently studied and deemed potentially successful in these ways is that of a game-theoretic architecture. It is technically possible, for example, to use mixed action-state deep reinforcement learning to detect and adapt to network intrusions with a 99%

true positive rate. However, the scope of AI-based cybersecurity can and has grown considerably to include many more threat vectors and activities on the blue side using an ever more advanced array of techniques and methodologies. What follows are many examples of such potential advancements, hubs able to help protect U.S. semiconductor manufacturing infrastructure. Given the sum total of these advances, one project alone is simply insufficient to build them all. As such, this paper is capable of delivering a taste and should be taken as emblematic rather than all-encompassing.

Threats to U.S. semiconductor manufacturing infrastructure are constantly evolving. But so are the technologies used to defend these facilities and systems. As an example, it is now possible to use only a few convolutional neural network layers to automate the identification of IoT malware in network packet data with a 99.7% true positive accuracy. Also, the use of GAN models is a rapidly growing field. A GAN model can operationalize a framework to automatically generate and test binary robust adversarial inputs against sensor data. That is, once the attacking GAN has learned how to produce adversarial inputs, the defending GAN starts producing data that is trained on the adversarial inputs from the attacking GAN. The process iterates between the opposing models until eventually neither model can improve, turning adversarial training into a kind of game. In other words, it is now possible to form two actually distinct subnetworks to vet malicious websites for large-scale cyber threats with 96.36% accuracy.

7.2. Potential Innovations in Semiconductor Security

7.2. Potential Innovations in Semiconductor Security

The previous section focused on ways to apply current cybersecurity solutions to the unique vulnerabilities in the U.S. semiconductor industry. But it is also useful to consider broadly what might be game-changing in the field of semiconductor security. What technologies, if available, might dramatically change our current understanding of cybersecurity and the security of integer overflow in particular?

Subsection 7.2 is focused on AI-enhanced cybersecurity. Although one of our S&T elements is specifically focused on this concept, the technology is developing rapidly, encompassing a broad range of products, strategies, and algorithms. The tools that characterize AI-enhanced cybersecurity all evaluate programs in situ in some way or

another, as software runs, rather than evaluating the authors or static code ahead of time that runs physically in a processor. Sections 7.2.1 through 7.2.3 describe in more detail how this basic approach can be melded into entire products, strategies, or algorithms. Ultimately, the hope in pursuing this programming for cybersecurity is that we can develop tools that "outmimic" the known defenses of malware like ZD3 TkE D4rkw3b that use dynamic checks to avoid detection until activation. These tools would need to generate new checks faster than adversaries can generate new evasions.

8. Conclusion and Recommendations

In recent years, several key industries and supply chain pipelines have become increasingly vulnerable to foreign and domestic cyber and physical attacks, creating new and growing risks and threats to U.S. safety, security, and economic well-being. This essay outlines several key techniques that can be incorporated into an AI-enhanced cybersecurity portfolio and how these can help safeguard critical systems that are now key in the manufacture of automated processes, components, and systems. Further, we also outline an industry-specific penetration path for cybersecurity solutions in the semiconductor manufacturing space via specific techniques designed to protect these systems and the techniques behind them in the discussions that follow. These techniques have been validated and extensively tested in real-world, real-time applications over a seven-year period of network-level Digital Twin-based production-level emulation.

Drawing from the operational deployment knowledge presented in this ongoing study, we provide the following recommendations for protecting the U.S. semiconductor manufacturing infrastructure:

- Execute a structured risk assessment for potential cyber-threats to manufacturing devices and their networks. This should include the damage that could be done by a successful cyber-attack as well as the potential financial impact on your organization.

- Employ the SecureChannel best practices discussed in this essay to help factories form secure trust relationships with partners, component suppliers, and OEMs.

- Institute automatic device insertion and registration at the network edge to ensure an auditable and fully traceable provenance policy for new remotely inserted assets.

- Employ secure management systems to give IT the ability to securely manage each and every device and its trustworthiness separately, as many devices are built by OEMs with no physical connection to the producing organization.

8.1. Key Findings and Takeaways

I. Key Findings We used our new AI model to generate state-centric scenarios of impactful and highly likely cyber-threats to U.S. semiconductor manufacturing. All identified scenarios involve non-physical phenomena, focus on competitive, industrial, and political domains, involve mostly foreign actors, and are the result of crime and espionage, with no involvement on the part of the US. Threat severity among these scenarios varies widely and depends on the specific industry sectors and assets targeted.

II. Takeaways A global superconductor company loses its competitive edge in sensitive sectors where industrial espionage between superconductor fabricators is direct, thus uncoverable, and the public true reason for the decline cannot be hidden. Industrial espionage or crime happens when others have a different "better" semiconductor statt. Any cyber-attack that causes an increase in cyber-insurance rates for the global semiconductor fabricator industry is likely the result of some criminal or national industrial espionage. US superconductor fabricator and foreign fab are merging, thus the national security risks are surely secretly known, very high, and significant. Non-semiconductor corners of semicon fabricators are worth their stock multiplier. Restrictionless insider stock selling opportunities depend on market perspective. A patent applied for predictive large-scale proposed new semiconductor product effort is likely to fail in 10 ASIC years.

8.2. Practical Recommendations for Industry Stakeholders

Next, industry stakeholders involved in U.S. semiconductor manufacturing are provided with recommendations and action steps based on the insights and results of the analyses presented in the essay.

These include chip fabs and other semiconductor manufacturing infrastructure providers; manufacturers of chip design tools, electronic design automation (EDA) software and services, computer-aided design (CAD) systems, and services; companies involved in software and hardware cybersecurity for system-level architectures and services. In addition to following these recommendations throughout the developing

applications discussed in this essay, industry representatives should consider and engage with discussions presented throughout.

First, chip fabs should critically examine the benefits of "black boxing" their operations and consider what security by obscurity could mean for them. Second, the industry at large must ensure appropriate levels of security, including effective penetration testing (red and blue teaming), so as not to provide a false sense of security to stakeholders and certify vulnerabilities by engaging ethical hackers. Third, those providing or developing real-time AI-enhanced intrusion detection and response systems (IDRS) must ask what must be done in the systems' design and implementation to make them trustable, both to parties that would interfere with its operating limits and those that would rely on it. MATLAB - despite its history of "bad behavior" by virtually coming to an abrupt stop - is not so easily replaced as a secure piece of operational software. Each of these provides some small insight into how a future research agenda might develop in this area.