Defending Autonomous Intelligent Systems Against Cyber and Electromagnetic Warfare Attacks

Nathaniel Poteat
Department of Computer Science and Information Systems
University of North Georgia, The Military College of Georgia
Dahlonega, GA 30597
ncpote0618@ung.edu

***Abstract*—Autonomous Intelligent Systems (AIS) is a rapidly growing interdisciplinary field at the intersection of various disciplines of engineering, science, and computer science that encompasses everything from autonomous vehicles to intelligent robots and even internet of things (IoT) devices. Because of their nature as cyber-physical devices, AIS' are vulnerable to both cyber and electromagnetic warfare (EW) attacks. These attacks can compromise personal safety, privacy, and even national security. The purpose of this research paper is to identify some of these cybersecurity, embedded, and EW vulnerabilities and provide inexpensive solutions using widely available resources such as artificial intelligence (AI) and software defined radios (SDRs).**

***Index Terms*—cybersecurity, electromagnetic warfare (EW), artificial intelligence (AI), software defined radio (SDR), autonomous intelligent systems (AIS), robotics, self-driving cars, unmanned aerial vehicles (UAV), drones**

I. Introduction

In recent years there have been numerous advancements in AI, computer vision, and robotics, and there has been an effort to bring these technologies together to create even more powerful systems. As is stands, everything from personal to industrial robots, autonomous vehicles such as self-driving cars, products with military or governmental applications such as drones or unmanned aerial vehicles (UAVs), to even IoT devices like smart fridges or Amazon Alexa can be considered autonomous intelligent systems. Just like any other electronic devices, these systems are not without vulnerabilities. On the hardware side of things, malicious actors can interfere with signals, tamper with the electronics, or immobilize these systems. On the software side of things, AISs are vulnerable to the standard range of cyber attacks, and they become more vulnerable the more connected and complex they are. They combine all the strengths of these separate technologies, but they also combine all the weaknesses and complexity they possess as well.

As the field of AISs continues to grow, it becomes even more important to identify and address their security vulnerabilities and requirements. This is especially important now because there has been a rising threat, greater scope, and a larger impact of cyber attacks from both state and non-state actors. For example, in June 2010, the 500-kilobyte Stuxnet worm was found to have infected the cyber-physical systems that controlled industrial and nuclear facilities in Iran and caused catastrophic damage to uranium-refining centrifuges [1]. Stuxnet propagated itself over highly secured and even air gapped networks and remained undetected by capturing a snapshot of normal operation over a period of time and playing it back as the virus compromised the programmable logic controllers (PLCs) and tore the centrifuges apart. This attack was believed to have been carried out by state actors and demonstrates how even air gapped cyber-physical systems - which AISs are - can be attacked. On a smaller scale, AISs such as self-driving cars can easily be exploited for under $100 using open-source software and and the OBD-II on-board diagnostic port as shown in [2].

As we have seen, Autonomous Intelligent Systems can extremely vulnerable, and the impact of being hacked can be catastrophic. It is possible for a smart home IoT device to be exploited and used to spy on people; It is possible for a self-driving car carrying a family to be remotely controlled by malicious actors. It is possible for industrial robots to be compromised and used to cause critical damage and loss of life. It is even possible for military drones to be hijacked and used against its own soldiers or made ineffective through signal jamming. The question becomes, how do we prevent this from happening?

This research provides a brief overview of AISs, discusses cyber, cyber-physical, and EW vulnerabilities, and proposes solutions to these vulnerabilities using AI and SDRs. This paper gives a brief history of AISs and defines it's components. Security Vulnerabilities is sub-divided into three sections: Cybersecurity, Cyber-Physical (Embedded), and Electromagnetic Warfare. This is followed by Solutions, where we focus on how AI and SDRs can help defend against attacks along those vectors. We finish with our conclusion.

II. Overview of Autonomous Intelligent Systems

Autonomous Intelligent Systems and its subsidiary fields have a long history. AI, for example, began as early as Greek philosophers attempted to rationalize systems that describe human intelligence, but it wasn't until 1956 when John McCarthy coined the term "artificial intelligence" [3] [4]. Autonomous Vehicles trace their lineage back to 1917 when the U.S. Army developed the first unmanned aerial vehicle (UAV) to search for German U-Boats. It took its first flight on March 6th, 1918. Since then, autonomous systems have increased in

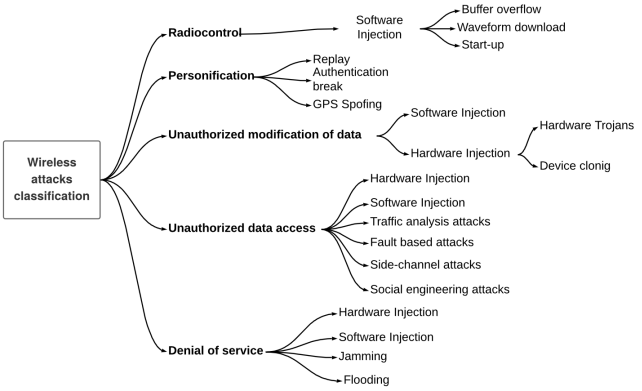

Fig. 1. Wireless attacks that can affect AISs [22]

complexity and have become an interdisciplinary field that borrows from engineering, computer science, biology, and more to implement physical controls and task/motion planning with reasoning and decision-making with high levels of autonomy and intelligence. Now, AISs are capable of adapting to weather, controlling systems, and making decisions with high levels of intelligence and autonomy.

AISs are inherently cyber-physical systems. In cyber-physical systems, the software controls the hardware. The security of the software component is critical to the functioning of the physical component and vice versa. Most modern CPSs rely on embedded systems which use Integrated Circuits (ICs), Field Programmable Gate Arrays (FPGAs), and Application Specific Integrated Circuits (ASICs) implemented with Programmable Logic Controllers (PLCs), microcontrollers, and microprocessors. Because of their nature, embedded systems must maintain security using limited resources - especially when connected to the internet [5]. Unlike traditional computer systems, CPSs are also at risk of EW attacks and physical damage. Thinking about security from an EW perspective requires a completely different mindset. EW can employ inexpensive technologies such as Software Defined Radios (SDRs) to conduct signal sniffing or jamming. Most security is focused on the cyber side of things because of traditional computers, but there isn't much knowledge on how to protect against physical and EW threats [6] [7].

III. Security Vulnerabilities

A. Cybersecurity

AISs are even more vulnerable to cyber attacks than traditional computing devices. Security measures such as firewalls and traditional antivirus software are not suitable for the cybersecurity conditions AISs face. They rely on limited computing power and resources due to their usually small form factors, specialized purposes, and autonomy. This becomes even more exacerbated as AISs become increasingly more connected to the IoT. The more AISs such as UAVs, robots, self-driving cars, and even toasters are connected to the Industrial, Medical, and especially the Battlefield IoT the more attack surface there is. In fact, the more critical the sector the device is in, the more likely it is to be attacked, leading to significant risks to public safety, national security, and economic stability.

Effective cybersecurity techniques focus on ensuring a system's confidentiality, integrity, and availability first and foremost. However, it would not be comprehensive cybersecurity without also ensuring authentication, non-repudiation, and privacy. As mentioned earlier, this becomes much more difficult in AISs which deploy embedded computing to make CPSs. Threats range from passive eavesdropping and data theft to active traffic analysis, spoofing, and service denial attacks, all of which pose significant challenges to the security of these systems. For a comprehensive list of cybersecurity vulnerabilities facing AISs and solutions outside the scope of this paper, please refer to [8].

One of the contributing factors to AIS cybersecurity vulnerabilities is that that their data communication is unsecure because of the focus on rapid development and resource efficiency. For example, the Robot Operating System (ROS) and similar AIS operating systems and frameworks were originally designed for research purposes. Because of this, ROS communication is unencrypted, unsecure, and lacks security features to prevent interception and spoofing of its communications between components of the system. An attacker can easily capture, read, and spoof ROS messages [9].

There's also the potential for an attacker to throw large amounts of resources against the AIS' limited resources during an attack. According to [10], attackers can conduct brute force and dictionary attacks while leveraging massive and relatively inexpensive cloud computing resources for acceleration.

To address these cybersecurity vulnerabilities, there is a need for more comprehensive, resource-efficient, and autonomous security measures.

B. Cyber-Physical (Embedded)

Most AIS' are implemented on embedded systems that control a physical system, hence the name Cyber Physical Systems. Because of their small form factor, mobility, and special purpose, AIS' must rely on limited processing power and resources. That, combined with the fact that these systems are often far from human supervision and under harsh environmental conditions makes it difficult to prevent both unauthorized cyber and physical access. AIS' typically do not have the computing resources needed to run traditional antivirus software and other conventional computing solutions. Embedded systems are usually composed of a CPU, RAM, ROM, and I/O interfaces. The more I/O hardware components, such as WiFi, Bluetooth, and USB, that can be connected to a system, the more vulnerable to attack. As a result, AIS' combine the cybersecurity issues of more conventional computing systems with the vulnerabilities and limitations of embedded and CPSs [5].

AIS' are also vulnerable to attacks that exploit vulnerabilities in the hardware and implementation of the system. Some of these attacks include hardware trojans, side channel attacks, and fault attacks that could lead to sensitive data loss

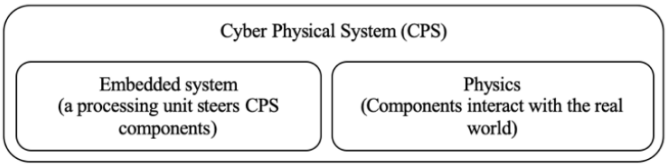

Fig. 2. Cyber-Physical (Embedded) System Diagram [5]

or system exploitation. Side channel attacks leverage internal knowledge about the underlying hardware and implementation of the system to exploit the software, and fault attacks force the system to perform under non-optimal conditions in order to manipulate the system [12]. Hardware trojans can be inserted into a system and remains dormant until triggered by specific conditions. This then allows attackers to gain unauthorized access [8]. Any of these attacks can occur when an attacker has physical access to the system such as during manufacturing, maintenance, or as a result of battlefield losses.

Another major consideration of AIS' is that they are often connected to the internet and to other devices to make the IoT. This introduces even more security complications by introducing more entry points to the system and thus increasing the attack surface. Being directly connected to the internet allows potentially anybody on the internet an attack vector, and if one of the AIS' in the IoT is more vulnerable than the others, then the entire network is only as strong as that AIS [5]. However, not having this interconnectivity introduces other security risks. For example, most operating system and firmware updates are transmitted over the internet, so keeping AIS' off the internet means that security updates will not install. At the same time, new updates introduce new features that provide new attack vectors for hackers [8].

One of the ways to counteract attacks is by reinforcing AIS resilience. Resilience means that a system is able to continue functioning as intended after a cyberattack or being disconnected from the operator. According to [5], several approaches to implement resilience include game theory, event-triggered control, mean subsequence reduced algorithms, and trust based approaches. This can also involve detecting and isolating attacks through observer-based techniques, analytical consistency, watermarking, baiting, and learning-based anomaly detection. More ways to implement resiliency in AISs that require high precision tracking for path tracking in an efficient and emerging way is to use Fuzzy Models and Event-Triggered Schemes (ETSs). Fuzzy Models allow AI to make decisions in a much more efficient and human-like way. ETSs only transmit signals when an event-triggered condition is met [12].

C. Electromagnetic Warfare

AIS security extends beyond the traditional cyber threats to encompass vulnerabilities in the Electromagnetic Spectrum (EMS). Electromagnetic Warfare (EW) encompasses any offensive and defensive actions that utilize the ES to intercept, analyze, and manipulate signals while protecting one's own use of the ES [13]. There are three primary subdomains of EW. These include Electronic Attack (EA), Electronic Support (ES), and Electronic Protection (EP).

Electronic Attack involves offensive actions and active monitoring within the EMS. One prominent tactic in EA is jamming, where attackers flood communication channels with interference to disrupt or degrade signal reception. There are many two main types of jamming: noise jamming and deceptive jamming. Noise jamming involves what we typically think of when we think about jamming. Noise jamming injects noise or interference into the EMS, and there are multiple subtypes of jamming including tone, sweep/barrage, and protocol-aware jamming which target specific frequencies or mimic communication protocols. Deceptive jamming manipulates or imitates a signal to cause deception, and includes range deception, velocity deception, and angle deception. In deceptive jamming, a false target may be generated to confuse an enemy radar, exploit a guidance system, or more [13] [8]. Jamming poses a significant threats to AISs by potentially rendering them incapable of receiving crucial commands or transmitting vital data.

Electronic Support entails passive monitoring of the EMS to gather intelligence or identify potential threats. Attackers can use ES techniques to gain insights on AIS operations and vulnerabilities by sniffing and analyzing radio frequency signals. They can then use this information to gather reconnaissance for future attacks [14].

Electronic Protection encompasses defensive measures aims at countering electronic attacks and safeguarding AISs against electromagnetic threats. Active Electronic Countermeasures (ECMs) involve the generation and transmission of EM energy to degrade the effectiveness of enemy EW systems. Techniques such as noise jamming and deceptive jamming disrupt adversary communications or create false targets to confuse enemy sensors. Passive ECMs, including chemical or mechanical defenses, fortify AISs against non-destructive attacks and information leakage [8] [10].

Employing EW techniques can be extremely inexpensive through the use of Software Defined Radios (SDRs) and open-source software. Commercially-available HackRF only costs about $300 and can operate in frequencies from 1MHz to 6GHz [15]. SDRs such as HackRF can facilitate signal jamming, sniffing, and spoofing. They can allow attackers to disrupt communications, intercept sensitive data, and manipulate AIS operations [14].

Using EW techniques and even inexpensive SDR platforms, attackers can exploit GPS vulnerabilities. Because the GPS protocol transparency, an attacker can sniff and spoof GPS signals and can lead to erroneous navigation and compromised mission objectives [15]. Open-source projects like GPS-SDR-SIM enable attackers to generate and transmit counterfeit GPS signals to undermine the reliability and accuracy of AIS navigation systems. Some countermeasures against GPS spoofing include real-time validation of GPS signals, encryption of navigation data, and the implementation of anti-spoofing EP

techniques to detect and mitigate fraudulent signals [15].

Additionally, the emergence of AI-aided EW techniques further exacerbates the threat landscape and empowers adversaries to deploy sophisticated attacks against AISs with unprecedented efficiency and stealth [13]. These techniques can identify and classify AISs based on unique identifiers such as MAC addresses, SSIDs, and traffic patterns.

Addressing vulnerabilities on the EMS requires a multifaceted approach that encompasses advanced encryption protocols, signal authentication mechanisms, and resilient communication architectures.

IV. Solutions

A. Artificial Intelligence

Because of the autonomous nature of AISs, they already possess AI capabilities to operate, communicate, and make decisions. The two types of AI are narrow/weak AI and General AI. Although narrow AI is trained on a small set of tasks and therefore more resource efficient, General AI can handle everything from controls to navigation to even the security and resilience of the system [16]. Leveraging AI-driven solutions can enhance threat detection, response capabilities, and overall resilience of AISs in dynamic and adversarial environments. However, there is a trade off between capabilities and resource utilization.

AI-powered cybersecurity systems excel at predictive intelligence by analyzing vast amounts of data from divers sources such as articles, news, and cyber threat research. By leveraging computational linguistics, these systems curate relevant information to identify emerging abnormalities, cyberattacks, and countermeasures. This proactive approach enables AISs to anticipate potential threats and allocate resources effectively [17]. AI-driven endpoint security solutions use recurrent training procedures to establish a behavioral baseline for endpoints. Any deviations from normal behavior can trigger alerts that enable proactive threat prevention and response mechanisms. By continuously adapting to evolving threat landscapes, AI-equipped AISs can detect and mitigate malware attacks in real-time and reduce the reliance on signature-based detection models [17]. Training ML algorithms on extensive datasets of intrusion fingerprints and attack patterns can enable AI systems to detect and attribute cyber intrusions as they happen. An AI-driven intrusion detection system (IDS) can analyze network traffic and system logs to identify anomalous activities that indicate potential security breaches. They can also potentially attribute attacks to specific threat actors by analyzing their tactics, techniques, and procedures (TTPs) [17].

Edge computing platforms equipped with AI-enabled intrusion detection systems offer real-time threat detection and response capabilities at the network perimeter. By offloading computational tasks to edge devices, AISs can mitigate latency issues and enhance security posture in distributed environments [18]

Deploying ML models on resource-constrained embedded systems presents unique challenges due to limited processing power and memory constraints. However, recent advancements in embedded machine learning algorithms and hardware accelerators offer promising solutions to address these challenges [19]. One of these ways is via hardware acceleration using FPGAs, GPUs, and ASICs. Each one offers advantages in terms of flexibility, computational performance, and energy efficiency [18].

Implementing the aforementioned AI-based solutions with the help of Fuzzy logic can help improve an AISs resilience by giving it more human-like decision-making abilities. Fuzzy models used Adversarial Neural Networks to attempt to mimic human decision-making when dealing with vague and imprecise information. Fuzzy Models are already widely used in radar and signal processing applications [13].

Cognitive radio technologies leverage AI algorithms to manage the EMS, adapt to changing environmental conditions, and mitigate interference in wireless communication systems. By employing ML techniques AISs can optimize spectrum utilization and enhance resilience against jamming and spoofing attacks [20].

AI-driven solutions hold immense potential for fortifying Autonomous Intelligent Systems against cyber and electronic warfare threats. By harnessing predictive analytics, anomaly detection, and adaptive response mechanisms, AISs can proactively defend against sophisticated adversaries and ensure mission-critical operations in challenging environments. However, the integration of AI technologies into AIS architectures necessitates careful consideration of resource constraints, hardware compatibility, and algorithmic efficiency to achieve optimal performance and security outcomes.

B. Software Defined Radio

Software Defined Radios (SDRs) have emerged as powerful yet inexpensive tools in the realm of defending autonomous intelligent systems (AISs) against cyber and electronic warfare (EW) attacks. A critical aspect of AIS defense lies in enabling autonomous responses to cyber and EW threats. [21] proposes triggers that prompt AISs to react autonomously in the face of threats, such as low battery levels or detected adversarial activities. By leveraging SDRs and machine learning algorithms, AISs can autonomously detect, identify, and mitigate signals indicative of cyber or EW threats, thereby bolstering their resilience and responsiveness.

The convergence of SDRs and AI to create cognitive radios shows immense promise in fortifying AISs against cyber and EW attacks. ML models deployed for cognitive radios can be trained to identify signals of interest (SOIs), mitigate interference, and optimize communication links. By employing ML-driven signal processing techniques, AISs can effectively navigate complex environments, adapt to dynamic threat landscapes, and maintain robust communication channels [21]. By leveraging AI-driven cognitive capabilities, SDR-based AISs can autonomously select optimal transmission parameters, detect and avoid jammed frequencies, and ensure seamless communication in contested environments [20]

[7] highlights the importance of full duplex communication enabled by SDRs in countering EW threats. By transmitting

and receiving signals simultaneously, AISs can create protective "shields" against jamming and interception attempts. Additionally, SDRs facilitate the implementation of electronic counter-countermeasure (EECM) techniques, including spatial, spectral, and temporal strategies, to thwart adversarial EW activities effectively.

By harnessing the versatility, agility, and intelligence of SDR technology, AISs can effectively mitigate cyber threats, counter EW attacks, and maintain operational resilience in challenging environments. Moreover, the synergistic integration of SDRs with AI-driven cognitive capabilities unlocks new avenues for autonomous decision-making, adaptive spectrum management, and dynamic response to evolving threats. As the landscape of cyber and EW warfare continues to evolve, SDR-based solutions remain at the forefront of defending autonomous systems against adversarial incursions.

V. Conclusion

Addressing the vulnerabilities inherent in Autonomous Intelligent Systems (AISs) necessitates the implementation of robust security measures. Artificial Intelligence (AI) technologies, in conjunction with Software-Defined Radios (SDRs), offer promising avenues to mitigate diverse security concerns. By harnessing AI capabilities, AISs can enhance their defensive capabilities, fortify secure networking protocols, uphold confidentiality, and deploy self-healing mechanisms to preempt, detect, and counter cyber and electronic warfare (EW) attacks. SDRs, on the other hand, provide the agility and versatility needed to configure secure communication networks, thereby combating threats such as reconnaissance, interception, and spoofing [8].

In response to the evolving threat landscape, collaboration between researchers and practitioners is paramount to develop comprehensive cybersecurity frameworks tailored to the unique requirements of AISs. This collaborative effort entails integrating advanced AI algorithms for intrusion detection, anomaly detection, and adaptive security measures. Furthermore, the adoption of secure communication protocols, robust encryption standards, and stringent access control mechanisms is imperative to safeguarding AISs against cyber and EW threats. By prioritizing cybersecurity throughout the lifecycle of AISs, from design and deployment to maintenance and updates, stakeholders can mitigate risks and ensure the resilience of autonomous systems in an increasingly hostile digital environment.

Despite significant strides in AI and SDR technologies, securing AISs remains an ongoing challenge that requires continuous research and innovation. As we delve deeper into the realm of multi-robot observation, software-defined networks, and inter-robot communications, additional areas for exploration and enhancement emerge.

References

[1] D. Kushner, "The real story of stuxnet," IEEE Spectr., vol. 50, no. 3, pp. 48–53, Mar. 2013, doi: 10.1109/MSPEC.2013.6471059.

[2] B. Payne, "Car Hacking: Accessing and Exploiting the CAN Bus Protocol," JCERP, vol. 1.

[3] M. I. Jordan, "Artificial Intelligence—The Revolution Hasn't Happened Yet," Harvard Data Science Review, vol. 1, no. 1, Jul. 2019, doi: 10.1162/99608f92.f06c6e61.

[4] J. Chen, J. Sun, and G. Wang, "From Unmanned Systems to Autonomous Intelligent Systems," Engineering, vol. 12, pp. 16–19, May 2022, doi: 10.1016/j.eng.2021.10.007.

[5] A. Aloseel, H. He, C. Shaw, and M. A. Khan, "Analytical Review of Cybersecurity for Embedded Systems," IEEE Access, vol. 9, pp. 961–982, 2021, doi: 10.1109/ACCESS.2020.3045972.

[6] K. Parlin, M. M. Alam, and Y. Le Moullec, "Jamming of UAV remote control systems using software defined radio," in 2018 International Conference on Military Communications and Information Systems (ICMCIS), Warsaw: IEEE, May 2018, pp. 1–6. doi: 10.1109/ICMCIS.2018.8398711.

[7] K. Parlin et al., "Full-Duplex Tactical Information and Electronic Warfare Systems," IEEE Commun. Mag., vol. 59, no. 8, pp. 73–79, Aug. 2021, doi: 10.1109/MCOM.001.2001139.

[8] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations," Int. J. Inf. Secur., vol. 21, no. 1, pp. 115–158, Feb. 2022, doi: 10.1007/s10207-021-00545-8.

[9] V. Matellán, J. Balsa, F. Casado García, C. Fernández, F. Martín, and F. Rodríguez Lera, Cybersecurity in Autonomous Systems: Evaluating the performance of hardening ROS. 2016.

[10] M. Kratky, V. Minarik, M. Sustr, and J. Ivan, "Electronic Warfare Methods Combatting UAVs," Adv. sci. technol. eng. syst. j., vol. 5, no. 6, pp. 447–454, Nov. 2020, doi: 10.25046/aj050653.

[11] B. Yuce, P. Schaumont, and M. Witteman, "Fault Attacks on Secure Embedded Software: Threats, Design and Evaluation," J Hardw Syst Secur, vol. 2, no. 2, pp. 111–130, Jun. 2018, doi: 10.1007/s41635-018-0038-1.

[12] Z. Lian, P. Shi, C.-C. Lim, and X. Yuan, "Fuzzy-Model-Based Lateral Control for Networked Autonomous Vehicle Systems Under Hybrid Cyber-Attacks," IEEE TRANSACTIONS ON CYBERNETICS, vol. 53, no. 4, 2023.

[13] P. Sharma, K. K. Sarma, and N. E. Mastorakis, "Artificial Intelligence Aided Electronic Warfare Systems- Recent Trends and Evolving Applications," IEEE Access, vol. 8, pp. 224761–224780, 2020, doi: 10.1109/ACCESS.2020.3044453.

[14] M. TajDini, V. Sokolov, and P. Skladannyi, "Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio," 2021.

[15] X.-C. Zheng and H.-M. Sun, "Hijacking Unmanned Aerial Vehicle by Exploiting Civil GPS Vulnerabilities Using Software-defined Radio," Sensors and Materials, vol. 32, no. 8, p. 2729, Aug. 2020, doi: 10.18494/SAM.2020.2783.

[16] R. E. Sylvertooth, "Assessing Security Architectures to Protect Against Malware in Embedded Narrow Artificial Intelligence Robots," Ph.D., Capitol Technology University, United States – Maryland. Accessed: Feb. 27, 2024. [Online]. Available: https://www.proquest.com/pqdtglobal/docview/2059254405/abstract/6D11CB7AAAD44

[17] I. A. Mohammed, "ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: A SYSTEMATIC MAPPING OF LITERATURE," SSRN Electronic Journal, vol. 7, pp. 172–176, Sep. 2020.

[18] Z. Zhang and J. Li, "A Review of Artificial Intelligence in Embedded Systems," Micromachines, vol. 14, no. 5, Art. no. 5, May 2023, doi: 10.3390/mi14050897.

[19] A. Biglari and W. Tang, "A Review of Embedded Machine Learning Based on Hardware, Application, and Sensing Scheme," Sensors, vol. 23, no. 4, Art. no. 4, Jan. 2023, doi: 10.3390/s23042131.

[20] S. Semendiai, Y. Tkach, M. Shelest, O. Korchenko, R. Ziubina, and O. Veselska, "Improving the Efficiency of UAV Communication Channels in the Context of Electronic Warfare," International Journal of Electronics and Telecommunications, pp. 727–732, Sep. 2023, doi: 10.24425/ijet.2023.147694.

[21] C. Manore, "Radio Frequency Spectrum Utilization on UAS for Long-Term Autonomous Missions," M.S., Northeastern University, United States – Massachusetts, 2023. Accessed: Feb. 27, 2024. [Online]. Available: https://www.proquest.com/pqdtglobal/docview/2808828533/abstract/3346789F75074E0

[22] J. de J. Rugeles Uribe, E. P. Guillen, and L. S. Cardoso, "A technical review of wireless security for the internet of things: Software defined radio perspective," Journal of King Saud University - Computer and

Information Sciences, vol. 34, no. 7, pp. 4122–4134, Jul. 2022, doi: 10.1016/j.jksuci.2021.04.003.