INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

Risk and Rewards:

Artificial Intelligence and Critical Infrastructure

Institute for Homeland Security

Sam Houston State University

Brooke Nodeland Ph.D.

Abstract

Artificial Intelligence (AI) is increasingly used by both public and private sector partners to advance cybersecurity best practice, however, the threat posed by these, and other contemporary threats cannot be understated. The threats posed by AI can be observed every day in email fraud, phishing attacks, and other types of malicious intrusion, with the potential for significant threats to more victims through larger scale attacks. There is further concern about AI tools being leveraged to directly target industrial critical infrastructures, including transportation, pipelines, energy, and other services whose networks are increasingly interconnected (Rinalidi, Peerenboom, & Kelly, 2001). Additionally, cyber threats from actors both foreign and domestic aimed at undermining public trust in government institutions, social cohesion, and the democratic process (Department of Homeland Security, 2023). Combined, these threats have the potential to wreak havoc on the American way of life.

Living off the land (LOTL) attacks have become the hallmark for AI based cyber-attacks and have been linked to disruptions in critical infrastructure services in the United States in abroad. LOTL techniques utilize existing legitimate network tools to carry out their attacks, and no longer require physical intrusion into a cyber network (Lenaerts-Bergmans, 2023). Since these attacks do not require an attacker to install any code or script within a target system, these types of attacks are more difficult to detect allowing hackers to remain undetected in a victim system's environment for an extended period of time (Lenaerts-Bergmans, 2023). These attacks pose a significant threat to critical infrastructure as they operate in industrial control and operational technology systems by essentially turning these systems against themselves (Parsons, 2023). These attacks are cheaper to respond to, are more difficult to detect, have higher success rates, require more rapid industrial response, and can have an immediate impact on safety (Parsons, 2023). These attacks can be used indiscriminately to attack any cyber based network.

These contemporary threats require that critical infrastructure providers use the most advanced human and machine-based responses to secure their networks and respond to these threats. Protecting industrial networks and systems, therefore, requires that AI be used responsibly and effectively to enhance the cybersecurity of the very systems that are being threatened. The following paper discusses the connection between AI and critical infrastructures, identifies significant threats posed by AI, as well as the use of AI in cybersecurity to secure essential networks in critical infrastructure.

Key words: artificial intelligence, critical infrastructure, living off the land, cyber security, cyber threats.

Introduction and overview

Almost overnight, we have found ourselves in the midst of an artificial intelligence (AI) revolution. AI is the technology behind this fourth industrial revolution and will profoundly impact the way we live (What, n.d.). AI uses advanced analytics and machine learning to create opportunities for technology-based products to engage in intelligent decision making, adaptability, and prediction. Almost daily, new innovations in AI, plans for advancement, and conversation surrounding the ways it is already prevalent in our daily activities, and in recent years, AI has increasingly been used to make everyday life simpler, with the technology found in the development of autonomous transportation, customer service chatbots, voice controlled virtual assistants such as Siri and Alexa, and navigation and travel applications such as Uber or Doordash. Despite this, less than half of Americans can identify AI's role in commonly used technologies even when they are aware of its presence (Kennedy, Tyson, & Saks, 2023). And while more than 27% of Americans report interacting with AI several times a day, the American public remains cautious about the impact of AI on everyday life (Kennedy et al., 2023). Between 2021 and 2023, for example, Americans reporting having more concern than excitement over the use of AI increased from 37% to 52% (Faverio & Tyson, 2023). Public support tends to be greater when AI is being used to facilitate daily tasks, and less supportive when it comes to methods that reduce the human element, such as in the workplace and healthcare, when it negatively impacts jobs, and regarding surveillance and privacy (Faverio & Tyson, 2023). While public concern appears to largely center on activities that might directly affect them, the largely scale uses and implications for advanced computing operations receives less attention, when in fact, the rapid advancement and proliferation of AI then, has been coupled with increasing concern surrounding the safe and responsible development and use of AI technologies. While the benefits of AI should not be discounted, the very real threat that is posed by the abuse of these technologies should also not be understated.

In the wrong hands, AI capabilities pose a significant threat to social cohesion and national security (Department of Homeland Security, 2023). In fact, few, if any technologies have ever been so uniquely situated to have such a profound impact as artificial intelligence processes that are being created today. The same technologies that are used to make our lives more convenient, can also be used to disrupt and destroy the networks and operations that we take for granted, and the threat of cyber physical attacks to basic household service providers is more prominent than ever (Department of Homeland Security, 2023). There are indications that AI based cyber threats are already being leveraged to directly target American industrial critical infrastructures including transportation, pipelines, energy, and other services whose networks are increasingly interconnected (Department of Homeland Security, 2023). Combined, these threats have the potential to wreak havoc on the American way of life by disrupting the delivery of daily services to American businesses and households (Exec.Order No. 14,110, 2023).

The United States has identified 16 critical infrastructures sectors that are considered so vital that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination of these effects (Critical infrastructure sectors, n.d.). These sectors have been identified as chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors/materials/waste, transportation systems, and water/wastewater (Critical infrastructure sectors, n.d.). AI technologies are an important component of security plans and practices for both public and private sector service providers around the globe, and careful attention is being given to how to leverage these processes to enhance daily operations, but also to detect, respond to, and mitigate the impact of cyber and cyber/physical attacks (Sakhnini, Karimipour, & Parizi, 2020). Cyber-attacks around the globe have drawn attention to the increasing use of AI based techniques, such as living off the land (LOTL) attacks. LOTL are AI based attacks and are unique in that they utilize existing programming within legitimate, authorized networks, making their presence difficult to detect and allowing cyber threat actors to remain in targeted victim networks for years without detection. In 2023 and 2024 alone, these approaches have been used both independently and in conjunction with physical attacks on critical infrastructures to disrupt daily life, for monetary gain, and to advance military standing against U.S. interests and in Russians war on Ukraine (Jasper, 2024).

In October 2023, President Biden issued an executive order calling for the responsible development of AI and directed the Department of Homeland Security to lead these efforts (Exec.Order No. 14,110, 2023), placing the highest urgency on governing AI development and taking steps to advancing a coordinated, federal government-wide approach. In addition, there is evidence suggesting that the implementation of machine learning algorithms increases the likelihood of the early prediction of system failures and cyber-attacks, significantly improving proactivity and security management in critical infrastructure (Govea et al., 2024). The following discussion provides a detailed review of the utilization of artificial intelligence in critical infrastructure operations and identifies significant AI based threats to these sectors. The discussion concludes by identifying steps that are currently being taken to utilize AI more effectively in defending critical sector networks and recommendations for the future to ensure that AI becomes a valuable cybersecurity tool and is used safely and responsibly to secure essential networks in critical infrastructure.

Problem statement

Concern surrounding the use of AI tools impacting national security vary from influencing the 2024 election; being misused in the development and production of chemical, biological, radiological, and nuclear weapons; as well as disruption and destruction of critical infrastructure systems, including transportation, pipelines and other services (Department of Homeland Security, 2023). Critical infrastructure systems, or critical systems (Laplante, Milojicic, Serebryakov, & Bennett, 2020) face significant cybersecurity threats, and the interconnected nature of these digital systems make them particularly vulnerable to cyberattacks from malicious actors aimed at infiltrating and disrupting essential systems (Yigit, Ferrag, Sarker, Maglaras, Chrysoulas, Moradpoor, & Janicke, 2024). Critical systems are those that directly affect public health, safety, and welfare and for which failure could cause loss of life, serious injury, or significant loss of assets or privacy" (Laplante et al., 2020:45), and include industrial services related to power generation and distribution, telecommunications, road and rail transportation, health care, banking, and more (Moteff & Parfomak, 2004). AI based cyber-attacks pose a significant threat to critical systems as they operate in industrial control and operational technology systems by essentially turning these systems against themselves (Parsons, 2023). Additionally, these attacks have higher success rates, require more rapid industrial response and can have an immediate impact on safety

(Parsons, 2023). These attacks can be used indiscriminately to attack any cyber based network and target significantly more victims through larger scale attacks (Schafer, 2024).

The threats posed by domestic and foreign adversaries are already being felt, marked by disruptions to American transportation networks, pipelines, and ports resulting from living off the land techniques which use flaws in the architecture and software implementation to gain access to accounts or create accounts that look like they should be part of the network (Ribeiro, 2024). And in February 2024, Cybersecurity & Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) issued a joint Cybersecurity Advisory (CSA) assessing state-sponsored cyber actors from the People's Republic of China (PRC), Volt Typhoon, as working to pre-position themselves on American IT networks for cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States (PRC state-sponsored, 2024). The advisory warns critical infrastructure organizations in the United States, as well as in several allied nations, that the threat of disruption or destruction to critical systems in the event of conflict between PRC and the U.S., is real and that Volt Typhoon has, in fact, already compromised the IT environments of multiple critical infrastructure organizations including in communications, energy, transportation systems, and water and wastewater system sectors (PRC state-sponsored, 2024). The threat posed by AI technologies cannot be understated. However, preparing for and responding to these attacks require that cybersecurity professionals, as well as all the public and private sector workforce responsible for operating critical systems, are all educated on the use of AI in securing these systems, primary threats for disrupting these systems, and utilizing the most advanced human and machine-based learning techniques to navigate and prevent these attacks in the future.

Topic discussion

The emergence of the internet of things (IoT) transformed the operations of traditional critical systems into more interconnected and intelligent systems allowing seamless communication and data exchange between various components of critical infrastructure (Raval, Jadav, Rathod, Tanwar, Vimal, & Yamsani, 2024). Critical infrastructures are connected in meaningful ways including physically, via cyber networks, geographically, and logically (Rinalidi, et al., 2001). The functional interdependency of these sectors, where the operation of one infrastructure is necessary for the operation of another (Zimmerman, 2001), makes securing these

critical systems vitally important to national security due to their susceptibility to cyber-attacks. Artificial intelligence has been defined as the science of making machines that can think like humans and do things that are considered "smart" (Pattam, 2021). Machines can process large amounts of data in ways different from the human brain, can do so more efficiently, and can do so without outside influence (Pattam, 2021). The ultimate goal is for AI to recognize patterns, make decisions, and make judgments in a similar manner to humans (Pattam, 2021), and to facilitate automation with intelligence (Raval et al., 2024). The breadth of the technology means that AI is used to serve a variety of purposes AI is used in AI is used by intelligence agencies to enhance cybersecurity, allowing them to sift through massive quantities of data and information more efficiently, such as through social media posts to identify potential threats as well as to identify terrorist threats and geopolitical activities. The ultimate goal is for AI to recognize patterns, make decisions, and make judgments in a similar manner as humans (Pattam, 2021), in other words, AI is used to facilitate automation with intelligence (Raval et al., 2024).

In 2024, AI is used to automate many mundane tasks that in the past would require humans to derive necessary information, to solve problems, and to combine real-time analysis with robust network communications structures to continually adapt to changing circumstances (Laplante et al., 2020). Machine learning (ML), a type of AI, is increasingly utilized in critical systems and allows computers to learn from data without being explicitly programmed (Alkhaleel, 2024). This technology is increasingly being used in the daily operation of critical systems including power grids and telecommunications networks. AI further has the capability to recognize patterns in human behavior and make assumptions about whether attempts to access a system or act within a system are valid or not (Raval et al., 2024). ML is used to increase the resilience of these systems and allow for continued operation of vital services in even in periods of disruption due to natural or man-made intentional attacks (Alkhaleel, 2024).

Applications of AI/ML in cybersecurity can mitigate emergent cyber threats in three ways: robustness, response, and resilience (Taddeo et al., 2019). AI can improve the capacity of a critical system to keep behaving as expected even when it processes erroneous inputs, or the systems robustness (Taddeo et al., 2019). System response can use AI to advance the capacity of a system to defeat an attack autonomously, to refine future strategies based on achieved success, and to possibly launch more aggressive counter operations each time the response is deployed (Taddeo et al., 2019). AI can increase the ability of a system to withstand an attack by enhancing threat and

anomaly detection, or system resilience. Some of the most common AI techniques used in cyber security include machine learning (ML), natural language processing, deep learning, reinforcement learning, computer vision, and expert systems. ML allows systems to learn from data without being explicitly told what to do with it, and can be used for malware detection, network intrusion detection, and anomaly detection (Rizvi, 2023). ML algorithms are trained to detect patterns and identify potential threats in large datasets that contain both benign and malicious traffic, or traffic that does and does not contain cyber threats (Merat & Almuhtadi, 2015). In recent years, machine learning has been used to detect suspicious behavior of supposedly legitimate users who use existing or create new accounts to engage in unauthorized activity on critical systems (Ribeiro, 2024). Natural language processing enables computers to understand and interpret human language and is used in cybersecurity to analyze unstructured data sources like social media feeds and online forums for potential threats (Rizvi, 2023). Deep learning, a subset of machine learning, uses deep neural networks to learn complex patterns from data for tasks such as malware detection, phishing detection, and fraud detection (Rizvi, 2023). Similarly, reinforcement learning is also a subset of machine learning that emphasizes judgment to train systems to decide how to respond to attacks based on the situation and the perceived level of the threat (Rizvi, 2023). Computer vision allows computers to interpret and analyze visual data as demonstrated in facial recognition and video surveillance (Rizvi, 2023). Expert systems mimic the decision-making capabilities of a human expert that are used for tasks like network intrusion detection and response and vulnerability assessment (Rizvi, 2023).

Then there is the threat posed by innovations in AI technologies as well. The very technologies and AI innovations we are working so hard to achieve, can ultimately be used against us if accessed or acquired by cyber adversaries, foreign or domestic (Vicens, 2024). In early 2024, FBI Director Christopher Wray described increasing concern surrounding the security of the AI models themselves, warning of the significant threats that would be posed if they were stolen (Vicens, 2024). And while AI is being used more than ever in the daily operation and security of critical systems, the same technology poses significant risk to these networks. For individual cyber threat actors, state-sponsored groups, and others who seek to cause harm or disrupt American lives, the tools to carry out AI based cyber attacks are more prevalent than ever. Increasingly, generative AI tools, similar to OpenAI but with a more deviant component, are made publicly available on the surface and dark web. These sites provide anyone with the programming code necessary to

wreak havoc on critical systems and disrupt daily business transactions and the life of millions of people (Schafer, 2024). For example, free hacker tools, such as WormGPT and FraudGPT, offer services free of safeguards that allows users to generate improved English-language phishing emails, generate code to spoof specific websites, and other requests for disruption to cyber networks (Ribeiro, 2024; Schafer, 2024).

AI is being used to enhance traditional and known methods of cyber-attacks. For example, traditional phishing email attacks might originate with a deceptive message designed in a way to make it appear as though it was being sent by a legitimate, or trusted, source such as a bank, work supervisor, or the U.S. postal service (Schafer, 2024). These messages were made to look like any other email the target would receive but were written with a sense of urgency requiring the recipient act quickly to avoid disruption to their services, ensure that their bank accounts, were secure, or respond to the needs of a supervisor. If the recipient were just quickly skimming through their email, they might just inadvertently click included links which would then either route them to a fake website or install malware on their device allowing the scammer to collect sensitive information provided by the victim, such as login credentials, financial details, or other personal data (Schafer, 2024). Traditional phishing attempts have become more common place and easily recognizable due to obvious mistakes such as incorrect email addresses, misspelled words, and misused phrases. But the expansion of AI tools has created even more opportunities for cyber treat actors to use these technologies to carry out more convincing, further reaching, profitable phishing emails, as well as made it easier to mass execute scams that are more convincing to potential victims (Schafer, 2024).

LOTL, sometimes referred to as living off the orchard, techniques involve abusing native digital tools and processes on computer systems to blend in with normal system activities and operate discreetly thereby lowering the likelihood of being detected, or blocked, because the tools are already deployed and trusted in the environment (CISA, 2024). These techniques make it harder for an existing system to identify their presence, making their identification and detection more challenging (Lenaerts-Bergmans, 2023). LOTL techniques also simplify the ease of carrying out a cyber-attack in that they use existing programming and do not require an intruder to create something new. Previously predominant malware attacks were more easily detected as their presence in a system was unwanted and did not align with allowed network activity, while the tools for a LOTL attack are already in critical systems for legitimate purposes, making them more

difficult to detect (Jasper, 2024). Deviant cyber actors have effectively used these techniques across multiple platforms including on-site, cloud, hybrid, Windows, Linux, and macOS (CISA, 2024). LOTL attacks are common in Windows operating systems as these operating systems are commonly used in corporate and enterprise settings where a significant number of people have authenticated access to the network and there are known vulnerabilities (CISA, 2024). Many organizations do not implement cybersecurity best practices that would support detection of malicious activity on their networks, making them ideal targets. When organizations do practice cybersecurity best practices, LOTL attacks remain difficult to identify because they use system programming that is supposed to be there for normal system operation (CISA, 2024).

LOTL attacks are a preferred technique among cyber threat actors because they use existing tools typically employed by authorized system users as opposed to deploying malware, and they do not leave traces of conventional signature-based indicators of their presence (Jasper, 2024). LOTL attacks have successfully been used to target critical systems in America and around the globe, with ongoing and continued threats posed by Chinese and Russian state-sponsored cyber groups. Russian threat actors have used LOTL attacks to enable cyber operations as part of the war Ukraine. These actors misused Windows-based software to archive stolen files by exploiting built-in system functionalities or external tools (Jasper, 2024). After entering systems through compromised routers, firewalls, and mail servers, Russian actors used a repeatable playbook through legitimate tolls for reconnaissance, lateral movement and data theft to limit detection of malware prior to deploying a wiper or other disruptive tool (Jasper, 2024). GRU, the Russian Chief Intelligence Office's, group Sandworm uses LOTL techniques extensively to attack Ukraine's critical infrastructure specifically. For example, they have created scheduled tasks or invoked encoded commands to execute ransomware payloads on transportation or logistics systems in Ukraine (Jasper, 2024). They have used operational technology to compromise Ukraine's energy grid, executing unauthorized control commands to switch off substations causing power outages to coincide with mass missile strikes on other critical infrastructure (Jasper, 2024). Domestically, the FBI has warned that Chinese government hackers are targeting water treatment plants, the electrical grid, transportation systems, and other critical infrastructures in the United States (Williams, 2024). In 2023, Microsoft released a public statement identifying People's Republic of China (PRC) state-sponsored Volt Typhoon as engaged in an active campaign to develop capabilities that could disrupt critical communications infrastructure between the U.S. and Asian

region during future crises (Microsoft Threat Intelligence, 2023). Volt Typhoon has targeted critical infrastructure organizations in Guam and the U.S. including communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and the education sectors (Microsoft Threat Intelligence, 2023). Volt Typhoon is known for their use of LOTL techniques when targeting CI, and private sector cybersecurity partners have found evidence of Volt Typhoons presence in CI network systems going back more than 5 years suggesting a relatively strong operational foothold on their network presence (People's, 2023).

Way forward

U.S. critical systems face significant and ongoing threat from the acceleration in advanced learning technologies, and we should already be taking steps to adapt and respond to these changes (Vicens, 2024). The unintended consequences associated with AI and other machine learning technologies have the capability to wreak havoc on the American way of life. The good news is that there is evidence that AI is already successfully being used to mitigate the threats posed by traditional cybercrimes such as network intrusion detection, malware detection, spam detection, and network traffic analysis (Sarker, Furhad, & Nowrozy, 2021), and they further enhance advanced cybersecurity practices, making critical systems more viable, secure, and difficult to infiltrate. And the diverse nature of AI can be found in existing cybersecurity approaches including facial recognition, biometrics, prediction, classification, and interpretive learning (Raval et al., 2024). In 2024, researchers exploring the integration and effectiveness of AI in improving the security of critical energy infrastructure, found an increase in the rate of cyber threat detection to 98%, and a reduction in incident response time by more than 70% (Govea et al., 2024). This demonstrates the effectiveness of AI in identifying and mitigating cyber risks both quickly and accurately (Govea et al., 2024). Predictive modeling uses AI to prevent cyber-attacks by recognizing potential threats before they occur and taking action to avoid them by assessing past attacks and detecting similarities (Rizvi, 2023). Integrating AI into critical infrastructure protection includes threat detection, as well as incident response and mitigation (Govea et al., 2024). Contemporary threats require that critical infrastructure providers use the most advanced human and machine-based responses to securing their cyber networks. AI systems can automate incident response to significantly reduce response time and minimize potential damage using real-time

decision-making algorithms to execute corrective actions and improving resilience of critical infrastructure (Govea et al., 2024; Rizvi, 2023).

As cyber-attacks increasingly use LOTL techniques, private and public entities must be equipped and prepared to respond to, and defend against, these network intrusions. Detecting unusual activity on these networks will require the use of behavioral analytics powered by AI and machine learning. One way to do this is to have plans in place to address the 'end-of-life' for commonly used hardware and software programs. The 'End-of-Life (EOL) date refers to the date when a technology, app, or product, including either soft- or hard-ware, is no longer supported by its manufacturer, and will no longer be actively upgraded or patched for vulnerabilities and/or security issues by the manufacturer/software creator (Understanding, 2023). EOL creates cyber security risk as devices or technologies become more vulnerable to attacks over time. While the continued use of these software can further cause compatibility issues and decreased system performance and productivity (Understanding, 2023), the bigger concern is that unwanted users can gain access to critical systems without detection and remain there for unknown periods of time.

The necessity of advancing cyber security practices to respond to, mitigate, and prevent AI based cyber-attacks on critical systems is of such concern to national leaders that in October 2023, President Biden issued an executive order calling for the responsible development of AI and directed the Department of Homeland Security to lead these efforts (Exec.Order No. 14,110, 2023), placing the highest urgency on governing AI development and taking steps toward advancing a coordinated, federal government-wide approach. Specifically, DHS was tasked with managing AI in critical infrastructure and cyberspace, promoting the adoption of AI safety standards globally, reducing the risks that AI can be used to create weapons of mass destruction, combatting AI-related intellectual property theft, and helping the United States attract and retain skilled talent (Exec.Order No. 14,110, 2023). The DHS is working with stakeholders both within and outside of the government to develop AI safety and security guidance to be used by owners and operators of critical infrastructure (Fact Sheet – Biden Harris). DHS also is looking at ways to capitalize on AI's potential to improve U.S. cyber defense. The Cybersecurity and Infrastructure Security Agency (CISA) actively uses AI and machine learning tools to detect and prevent cyber threats as well as assess the vulnerability of government cyber systems (Fact Sheet, 2024).

The monumental detection of Volt Typhoon's long-term presence in critical systems through LOTL attacks prompted policy changes impacting both public and private critical sectors

to enhance their cybersecurity practices. In February 2024, CISA in conjunction with the NSA, FBI, and other national and international cyber security agencies released an advisory to warn critical infrastructure organizations about the continued threat posed by this and other groups, and identified specific steps to mitigate Volt Typhoon activity (PRC state-sponsored, 2024):

1. Apply patches for internet-facing systems by prioritizing patching critical vulnerabilities in appliances (e.g. VPNs, firewalls, and routers) known to be frequently exploited by Volt Typhoon.
2. Implement phishing-resistant multi-factor authentication (MFA) account login in processes such as FIDO/WebAuthn authentication or public key infrastructure (PKI)-based.
3. Ensure logging is turned on for application, access, and security logs and store logs in a central system.
4. Plan “end of life” for technology beyond manufacturer’s supported lifecycle.

Recognizing that the prevention of LOTL attacks is difficult, these agencies provided additional guidance for organizations to best position themselves to detect and mitigate any damages resulting from LOTL attacks. Best practices for detection best practices include (CISA, 2024):

- Implementing detailed logging and aggregate logs in an out-of-band, centralized location that is write-once, read-many to avoid the risk of attackers modifying or erasing logs.
- Establishing and continuously maintaining baselines of network, user, administrative, and application activity and least privilege restrictions.
- Building or acquiring automation (such as machine learning models) to continually review all logs to compare current activities against established behavioral baselines and alert on specified anomalies.
- Reducing alert noise by fine-tuning via priority (urgency and severity) and continuously reviewing detections based on trending activity.
- Leveraging user and entity behavior analytics (UEBA), rather make use of machine learning to detect anomalies in user and device behavior.

Automated incident response systems are an important function of artificial intelligence in cybersecurity as these systems can perform several of these tasks including evaluating data,

identifying potential risks, and then working to contain or mitigate an attack, minimizing damage and disruption (Rizvi, 2023). CISA and partners (2024) make further recommendations for hardening critical systems to make LOTL attacks more difficult to carry out:

- Applying and consulting vendor-recommended guidance for security hardening.
- Implementing application allowlisting and monitoring use of common LOLBins (e.g. living off the land binaries or legitimate, built-in system binaries or processes to execute malicious activities).
- Enhancing IT and OT network segmentation and monitoring.
- Implementing authentication and authorization controls for all human-to-software and software-to-software interactions regardless of network location.

Finally, additional activities that critical sector administrators and cybersecurity professionals should be taking to ensure the reliability of critical infrastructures are extensive. For example, Yigit and colleagues (2024) recommend implementing an all-hazards approach to risk management that considers both cyber and physical threats to critical infrastructure integrity. The integration of incident response strategies with business continuity planning is recommended to ensure seamless continuity of operations during and after security incidents (Yigit, 2024). Critical sectors should regularly assess the security status of CNIs (e.g., container network interfaces) and conduct penetration testing to identify vulnerabilities and weaknesses in critical systems (Yigit, 2024). Other recommendations include using robust security mitigation measures such as intrusion detection systems, cryptography methods, firewalls, anti-virus software, and emerging security technologies like Blockchain, Artificial Intelligence (AI), and machine learning (Adil et al., 2022; Alyahya et al., 2022; Bellare et al., 1996), establishing and enforcing policies for maintaining and updating software and hardware, providing comprehensive cybersecurity training to all staff, and collaborating with industry experts and sharing threat intelligence (Yigit, 2024).

President Biden's 2023 Executive order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, recognizes the necessity of developing and using AI to ensure national security and protect American critical infrastructures and the importance of doing so safely and responsibly:

> Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure. At the same time,

> irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security. Harnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks. This endeavor demands a society-wide effort that includes government, the private sector, academia, and civil society.

The benefits of AI in everyday life as well as in the operation and security of critical infrastructure systems. The use of AI-enabled software tools to strengthen cyber defense demands that the responsible, ethical and safe use of these technologies and will us to assess and assist secure by design AI-based software adoption as well as assess and mitigate AI threats facing critical infrastructure (CISA, n,d,). Despite the benefits and progress marked by AI technology, the potential for the abuse of AI tools will continue to evolve and be exploited by cyber threat actors aiming to cause harm or disruption to the United States. It is imperative that public and private critical infrastructure operators work together to utilize these technologies safely and responsibly.

References

Adil, M., Khan, M. K., Jadoon, M. M., Attique, M., Song, H., & Farouk, A. (2022). An AI-enabled hybrid lightweight Authentication scheme for intelligent IoMT based cyber-physical systems. *IEEE Transactions on Network Science and Engineering*. https://doi.org/10.1109/TNSE.2022.3159526

Alkhaleel, B. A. (2023). Machine learning applications in the resilience of interdependent critical infrastructure systems—A systematic literature review. *International Journal of Critical Infrastructure Protection*, 100646. https://doi.org/10.1016/j.ijcip.2023.100646

Alyahya, S., Khan, W. U., Ahmed, S., Marwat, S. N. K., & Habib, S. (2022). Cyber secure framework for smart agriculture: Robust and tamper-resistant authentication scheme for IoT devices. *Electronics*, 11(6), 963. https://doi.org/10.3390/electronics11060963

Bellare, M., Canetti, R., & Krawczyk, H. (1996). Keying hash functions for message authentication. In *Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16* (pp. 1-15). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-68697-5_1

Critical Infrastructure Sectors. (n.d.). *Cybersecurity & Infrastructure Security Agency*. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Cybersecurity and Infrastructure Security Agency. (n.d.). *Artificial Intelligence*. https://www.cisa.gov/ai

Cybersecurity & Infrastructure Security Agency (CISA). (2024). *Joint Guidance: Identifying and Mitigating Living Off the Land Techniques*. https://www.cisa.gov/sites/default/files/2024-02/Joint-Guidance-Identifying-and-Mitigating-LOTL_V3508c.pdf

Department of Homeland Security 2024 Homeland Threat Assessment. (2023). *U.S. Department of Homeland Security*. https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf

Exec. Order No. 14,110, 3 C.F.R. 88 (2023). https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf

FACT SHEET: Biden-Harris Administration Announces New National Security Memorandum on Critical Infrastructure. (2024, April 30). *The White House.* https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/30/fact-sheet-biden-harris-administration-announces-new-national-security-memorandum-on-critical-infrastructure/

Faverio, M., & Tyson, A. (2023, November 21). What the data says about Americans' views of artificial intelligence. *Pew Research Center*. https://www.pewresearch.org/short-reads/2023/11/21/what-the-data-says-about-americans-views-of-artificial-intelligence/

Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence. *Systems*, 12(5), 165. https://doi.org/10.3390/systems12050165

Jasper, S. (2024, May 1). Chinese and Russian Legitimate Tool Attacks Mandate AI-Enabled Cyber Defenses. *The Cyber Edge by Signal*. https://www.afcea.org/signal-media/cyber-edge/chinese-and-russian-legitimate-tool-attacks-mandate-ai-enabled-cyber

Kennedy, B., & Tyson, A. (2023, February 15). Public Awareness of Artificial Intelligence in Everyday Activities. *Pew Research Center*. https://www.pewresearch.org/science/2023/02/15/public-awareness-of-artificial-intelligence-in-everyday-activities/

Laplante, P., Milojicic, D., Serebryakov, S., Bennett, D. (2020). AI and Critical System From Hype to Reality. U.S. Department of Energy Office of Scientific and Technical Information. https://www.osti.gov/servlets/purl/1713282.

Lenaerts-Bergmans, B. (2023, February 22). What Are Living Off the Land (LOTL) Attacks?. *Crowdstrike*. https://www.crowdstrike.com/cybersecurity-101/living-off-the-land-attacks-lotl/

Merat, S., & Almuhtadi, W. (2015). Artificial intelligence application for improving cyber-security acquirement. *Canadian Conference on Electrical and Computer Engineering, 2015-June*(June), 1445–1450. https://doi.org/10.1109/CCECE.2015.7129493

Microsoft Threat Intelligence. (2023, May 24). Volt Typhoon targets US critical infrastructure with living-off-the-land techniques. *Microsoft*. https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

Moteff, J. D., Parfomak, P., & Resources, Science, and Industry Division. (2004, October). Critical infrastructure and key assets: definition and identification. Washington: Congressional Research Service, Library of Congress. https://sgp.fas.org/crs/RL32631.pdf

Parsons, D. (2023, October 10). Living Off the Land Attacks and Countermeasures in Industrial Control Systems. *SANS*. https://www.sans.org/blog/living-off-land-attacks-countermeasures-industrial-control-systems/

Pattam, A. (2021, September 16). Artificial Intelligence, defined in simple terms. HCLTech. https://www.hcltech.com/blogs/artificial-intelligence-defined-simple-terms#:~:text=Artificial%20intelligence%20is%20the%20science,decisions%2C%20and%20judge%20like%20humans.

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection. (2023, May 24). *Cybersecurity & Infrastructure Security Agency*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. (2024, February 7). *Cybersecurity & Infrastructure Security Agency*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Raval, K. J., Jadav, N. K., Rathod, T., Tanwar, S., Vimal, V., & Yamsani, N. (2024). A survey on safeguarding critical infrastructures: Attacks, AI security, and future directions. *International Journal of Critical Infrastructure Protection*, 44: 100647. https://doi.org/10.1016/j.ijcip.2023.100647

Ribeiro, A. (2024, January 12). Senior US cybersecurity official reveals use of AI to counter hackers targeting critical infrastructure. *Industrial Cyber*. https://industrialcyber.co/critical-infrastructure/senior-us-cybersecurity-official-reveals-use-of-ai-to-counter-hackers-targeting-critical-infrastructure/

Rinalidi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE control systems magazine*, 21(6), 11-25. https://doi.org/10.1109/37.969131

Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science*, 10(5). https://creativecommons.org/licenses/by/4.0/

Sakhnini, J., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). AI and security of critical infrastructure. *Handbook of Big Data Privacy*, 7-36. https://doi.org/10.1007/978-3-030-38557-6_2

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cyber security: an overview, security intelligence modelling and research directions. *SN Comput Sci* 2 (3). https://doi.org/10.1007/s42979-021-00557-0

Schafer, N. (2024, April 11). The golden age of scammers: AI-powered phishing. *Sinch Mailgun*. https://www.mailgun.com/blog/email/ai-phishing/#chapter-2

Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), 557-560. https://doi.org/10.1038/s42256-019-0109-1

Understanding Patches and Software Updates. (2023, February 23). *Cybersecurity & Infrastructure Security Agency*. https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates

Vicens, A. (2024, March 11). Intelligence officials warn pace of innovation in AI threatens US. *Cyberscoop*. https://cyberscoop.com/intelligence-national-security-artificial-intelligence-threats/

What is the artificial intelligence revolution and why does it matter to your business? (.n.d.). *WIZ.AI*. https://www.wiz.ai/what-is-the-artificial-intelligence-revolution-and-why-does-it-matter-to-your-business/

Williams, K. (2024, March 3). 'Cyber-physical attacks' fueled by AI are a growing threat, experts say. *CNBC*. https://www.cnbc.com/2024/03/03/cyber-physical-attacks-fueled-by-ai-are-a-growing-threat-experts-say.html

Yigit, Y., Ferrag, M. A., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., Moradpoor, N., & Janicke, H. (2024). Critical infrastructure protection: Generative ai, challenges, and opportunities. *arXiv preprint arXiv:2405.04874.* https://arxiv.org/pdf/2405.04874

Zimmerman, R. (2001). Social implications of infrastructure network interactions. *Journal of urban technology*, 8(3), 97-119. https://doi.org/10.1080/106307301753430764

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Nodeland, Brooke Ph.D. (2024) Risk and Rewards: Artificial Intelligence and Critical Infrastructure (Report No. IHS/CR-2024-1014). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/5DGB8