Cybersecurity Recommendations for Confronting the Army's Industrial Internet of Things Challenges

By Maj. Allyson Hauptman

When the 2021 attacks on the Colonial Pipeline shut down petroleum delivery for five days, it sent the U.S. into an immediate gas shortage (Beerman, 2023). Analysis of the attack showed that this incident belongs on the long list of attacks on critical infrastructures that have been made possible by negligent attitudes towards cybersecurity and poor device management processes. Recently, the U.S. has seen an evolution in attacks on critical infrastructure, where attackers have been able to exploit vulnerabilities in information technology systems to gain access to operational technologies (OT) and cause damaging and disruptive effects to the physical systems themselves (Lehto, 2022). With the pedal to the metal on updating decades-old equipment to operate in the age of the internet, the nation must consider quick and effective methods to better secure that equipment.

Graphic by Isabel S. Wences.

The Army should be heavily invested in this process for multiple reasons, including its role in Defense support of civil authorities and responsibility to various critical infrastructure sectors reliant on the U.S. Army Corps of Engineers (USACE). Here, at the Army Cyber Institute (ACI), we are spearheading research and practice for the protection of critical infrastructure with an emphasis on critical infrastructure resilience (Fontes, 2020). As we explore ways to do this, it has become apparent that the most immediate and effective way for the Army to protect critical infrastructure within its control is not some new technological innovation or complex program. Rather, it is through better cybersecurity management practices that ensure Army personnel are a part of the solution, not part of the problem.

Previous administrations have emphasized the need for a whole-of-government approach to defending critical infrastructure. The Cybersecurity and Infrastructure Agency (CISA) has defined critical infrastructure as consisting of sixteen distinct sectors (Sectors, 2020). Many of these sectors rely upon the OT found in cyber-physical systems to manage physical processes, which include industrial control systems (ICS), distributed control systems (DSC), and supervisory control and data acquisition systems (SCADA). Many of these systems have been designed to operate in an air-gapped fashion, which helps protect the systems from dangerous intrusions. SCADA systems enable remote control over industrial processes, usually over wide area networks (WANs). Over the last two decades, these networks have transitioned from being relatively isolated to more integrated with IT networks using standardized protocols, a transition being expedited by the Industrial Internet of Things (IIoT) revolution. IIoT is the transition of industrial technologies to operate with more interconnectivity, automation, and artificial intelligence (Munirathinam, 2020). While IIoT promises to ease management overhead and create more efficient, data-driven processes for critical infrastructure, it can also significantly increase the risk of exploitation and compromise to OT which did not consider cybersecurity in its design.

The IT security principles that cyber professionals learn to prioritize clash with OT priorities. In many critical infrastructure sectors, such as

energy, availability is king. Such an emphasis is understandable, as continuity of service is of paramount importance. Unfortunately, this has also created an *if it ain't broke, don't fix it* mentality that has resulted in the continued operations of systems that are either behind multiple patch cycles or still in use, despite being past their manufacturer's end-of-life (EoL) date. For a recent example, in 2021 attackers were able to gain access to the Oldsmar, Florida water treatment SCADA system by exploiting an outdated operating system (Greenberg, 2021). Patch management is often associated with downtime, and thus it is easy for operators to prioritize availability over what they think is an unnecessary patch. In practice, this means that the patches deemed necessary are the ones that address a function issue, rather than a security one. While IT networks typically plan for managed downtime, this is not true for most SCADA networks, which were built to maximize uptime. This emphasis on uptime extends to legacy systems, where a system that is no longer supported by the manufacturer but still does its job is left in place until there is a function issue. This is exemplified by the 2024 Inspector General audit of the DoD's Development and Maintenance of Digital Modernization Strategy, which found the DoD is far from meeting all four of the strategy's goals, including the employment of up-to-date systems (DODIG, 2024).

There are several reasons why these legacy systems remain in place, including the expense of replacing legacy hardware, and the fear of disrupting operations. For sectors concerned with near 100 percent availability, these may seem like legitimate reasons for delinquent patches and the use of legacy systems; however, IIoT changes the game. Security assessments generally calculate risk as the product of the likelihood and consequence of a vulnerability being exploited. Before IIoT, the likelihood of exploitation appeared small, as the devices were relatively isolated from the rest of the world. Even SCADA networks were designed to be segmented with very restricted access. As IT and OT networks integrate, and the number of devices that touch a critical infrastructure organization's network increases, the likelihood of a vulnerability being exploited increases dramatically. Reasonably, organizations are not only afraid of time to apply patches, but also that untested patches may disrupt operations, a fear fueled by the recent CrowdStrike update (George, 2024).

Organizations concerned with high availability generally err on the side of giving employees more permissions than they need, including access to management accounts. Multiple employees are given duplicative privileges in order to ensure continuity of service (i.e. if one employee is sick, on vacation, or suddenly terminated, there are immediate back-ups with all the same accesses). Multiple vulnerability assessments of critical infrastructure network systems performed by Army teams revealed that many organizations were using shared credentials with a known password, and a survey of SCADA exploits revealed default credentials to be one of the primary exploited vulnerabilities (Larkin, 2014). This is not only an access concern, but an auditing one as well, because it makes it difficult to discern the source of an intrusion.

Recent advancements in AI technologies have significantly added to the drive to build out IIoT capabilities. These IIoT solutions rely on security tools such as virtual private networks (VPNs) to ensure confidential, authorized access to the organization's network. While these tools enable increased efficiency and auditing, they also increase the number of pathways into the network for an attacker. As more employees are permitted to use these remote access tools, careful monitoring of user accounts and permissions will become increasingly difficult, as shown by their exploitation in the Colonial Pipeline case. In this case, the attacker's initial entry point into the network was through a retired employee's VPN account that did not have two-factor authentication enabled.

This example represents one type of insider threat, where the employee himself was not the threat, but the vacancy he left allowed the attacker to assume his role and access. Malicious or former employees are an even more dangerous type of insider threat. Studies show that most insider threats did not join a company with ill intent; rather, some life event encourages them to utilize the knowledge they've gained as an employee to their advantage during or post-employment. This

was the case in the cyber-attack on Five Water Utilities in 2014, where a fired engineer was able to access the station network weeks later and perform a series of malicious activities using his knowledge of the network (Hassanzadeh, 2020).

The risks of account exploitation by both outside actors and insider threats increase even further when the devices used to connect to the network are part of a Bring Your Own Device (BYOD) model. BYOD allows users to hook their potentially untested personal devices up to a network for personal or professional purposes. While BYOD has several advantages, it is incredibly dangerous for critical infrastructure, particularly if the network touches OT devices. Research has shown that one of the main attack vectors attackers pursue to reach an organization's OT is to exploit a device that intermittently connects to the business IT network. Once they gain access to the device, attackers can pivot through downstream control devices and systems. A vulnerable personal device that intermittently connects to the IT network is an ideal way to do that, as evidenced by the exploitation of a water treatment plant network in Harrisburg in 2006, where the attackers planted a virus on an employee's laptop which was later connected to the plant's internal network (Hacker, 2006).

All this to say that the IIoT revolution has turned prior sketchy, but acceptable, practices into dangerous vulnerabilities for national critical infrastructure. Furthermore, the Army faces unique challenges in confronting them. Many of these challenges are rooted in Army personnel using the same types of negligent and unsecure practices outlined above. An immediate and effective way that the Army can overcome these challenges is through the proper application of cybersecurity management practices. In this final section, I will provide three challenges and recommendations for the Army as it embraces the IIoT revolution.

Challenge 1: Guarding Against the Insider Threat

The insider threat is one the Army must be particularly concerned over due to its model of frequent job rotation. As Soldiers move between duty positions and duty locations, they gain network and facility access required to fill their new roles. Unfortunately, while organizations are encouraged to promptly get new personnel all the accesses they need to do their job, there is much less motivation to ensure that those accesses are removed once they are no longer required. This is further exacerbated by the Army's "additional duties" programs, where Soldiers are assigned additional responsibilities that are not tied to their duty position or MOS. A key aspect of minimizing a sector's vulnerabilities to these insiders is to ensure that organizations are utilizing an adequate access model that limits employee permissions to the lowest level necessary. One way to do this is through access control models that are tied to a user's assigned role, as opposed to the user themselves. A user might have more than one role, but as soon as they are removed from one of those roles, they automatically lose all privileges associated with that role.

Recommendation: The Army should require role-based access control models for all critical infrastructure networks.

Challenge 2: Securing Intermittent Devices

As IT and OT networks merge, the vulnerabilities of the IT network become vulnerabilities to the OT network, and the security of the connected devices is dependent upon the security of all the other devices. In a post-COVID world, BYOD models are no longer just about enabling personal activities. The Army has rolled out several programs to enable teleworking and distributed work, particularly for email, messaging, and file sharing. While this may be appropriate for some portions of the Army's networks, BYOD presents too many risks to unpatched, outdated, sensitive critical infrastructure systems. Many components of the Army and the DoD utilize corporate-owned models, such as Corporate Owned Business Only (COBO) and Corporate Owned Personally Enabled (COPE). In a COBO model, the business owns and strictly limits the usage of the device, and users are only permitted to use it for specific work purposes. In a COPE model, the business owns and controls the device, but users may perform limited personal activities on the device. Despite the increased IT cost for the organization, both models offer significant security advantages over a pure BYOD policy. Foremost,

because the organization owns the devices, it can incorporate them into a patch management plan, thus preventing vulnerabilities caused by unpatched operating systems and applications. Additionally, it allows the organization to whitelist the devices that are permitted to connect to specific portions of the network, helping to limit unauthorized access.

Recommendation: The Army should require the use of COBO or COPE models for critical infrastructure networks.

Challenge 3: Adding Cybersecurity to Resiliency Strategies

The DoD has numerous policies in place to enhance the resiliency of critical infrastructure, including the energy resiliency of DoD installations. The DoD is the largest consumer of energy in the United States, which has pushed it to pursue more independent, renewable energy sources with the goal of having microgrids power all military bases (Hitchens, 2024). Furthermore, the U.S. Army accounts for over one-third of the DoD's energy consumption. While installing microgrids at Army installations would enable increased energy independence and security, their deployment comes hand-in-hand with the use of IIoT technologies for remote management. Beyond generating energy, these microgrids include tertiary layers that aid in the operation and control of other critical infrastructure facilities, such as transportation, communications, waste treatment, and healthcare.

The exploitation of such a grid through an IIoT vulnerability could be catastrophic as the effects cascade along several sectors. Resiliency assessments of military microgrids have largely focused on external effects on the grid with minimal consideration and testing for cybersecurity threats (Peterson, 2021). An unfortunate reality that IIoT security must consider is that adding traditional IoT security mechanisms on top of networks connected to OT may be both ineffective and disruptive, due to the limitations of legacy devices and systems. Recent research has shown that an effective way to identify and guard against vulnerabilities in IIoT networks is to utilize security by design principles, which consider and implement controls at various stages (Mouratidis, 2018).

Recommendation: The Army should require microgrids on military installations to adhere to security-by-design principles and test those principles in resiliency assessment.

About the Author

Maj. Allyson Hauptman is a Research Scientist at the Army Cyber Institute working in the Law, Policy & Strategy Division. She holds a Ph.D. in Human-Centered Computing from Clemson University and a Master's in Cyber Security from Tallinn University of Technology. She is a Cyber Operations Officer (17A) who has served as a Mission Element Lead in the Cyber Protection Brigade and a Company Commander in the 915th Cyber Warfare Battalion (now 11th CY BN).

References

Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023, May). A review of colonial pipeline ransomware attack. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)* (pp. 8-15). IEEE.

Department of Defense Office of the Inspector General (2024, July 9). *Audit of the DoD's Development and Maintenance of the Digital Modernization Strategy*.

Fontes, R. L., Korn, E., Fletcher, D., Hillman, J., Mitchell, E., & Whitham, S. (2020). Jack Voltaic®. *The Cyber Defense Review*, *5*(3), 45-56.

George, A. S. (2024). When trust fails: Examining systemic risk in the digital economy from the 2024 crowdstrike outage. *Partners Universal Multidisciplinary Research Journal*, *1*(2), 134-152.

Greenberg, Andy (2021, February 8). *A Hacker Tried to Poison a Florida City's Water Supply, Officials Say*. Wired. https://www.wired.com/story/oldsmar-florida-water-utility-hack/

Hacker hits Pennsylvania water system (2006, October 31). United Press International. https://www.upi.com/Top_News/2006/10/31/Hacker-hits-Pennsylvania-water-system/52641162318902/

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, *146*(5), 03120003.

Hitchens, Kathy (2024, October 1). *Leading the Change: 3 Army Installations Launch Microgrids*. Microgrid Knowledge. https://www.microgridknowledge.com/military-microgrids/article/55166408/leading-the-charge-3-army-installations-launch-pioneering-microgrids

Larkin, R. D., Lopez Jr, J., Butts, J. W., & Grimaila, M. R. (2014). Evaluation of security solutions in the SCADA environment. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *45*(1), 38-53.

Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer International Publishing.

Mouratidis, H., & Diamantopoulou, V. (2018). A security analysis method for industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *14*(9), 4093-4100.

Munirathinam, S. (2020). Industry 4.0: Industrial internet of things (IIOT). In *Advances in computers* (Vol. 117, No. 1, pp. 129-164). Elsevier.

Peterson, C. J., Van Bossuyt, D. L., Giachetti, R. E., & Oriti, G. (2021). Analyzing mission impact of military installations microgrid for resilience. *Systems*, *9*(3), 69.

Sectors, C. I. (2020). Critical Infrastructure Sectors. *Cybersecurity & Infrastructure Security Agency*.