DAY ONE PROJECT

Using "Wargaming" to Evaluate Manufacturing Cyberthreats and Ensure Supply-Chain Cybersecurity

Bill Barkman
Rich Taylor
Dennis Miller

July 2021

Summary

Small to medium-sized manufacturing (SMM) companies are the backbone of the U.S. industrial base. However, they do not have the financial or technical resources needed to protect themselves from cyberthreats such as computer hacking, embedded malicious software, and "internet of things" sensors sending sensitive information to foreign counties. These cyberthreats can cause huge damage to the U.S. economy and national security. With relatively limited investment, cybercriminals can disrupt critical supply chains, damage key sectors, and delete or corrupt important information resources.

The Biden-Harris administration should address these threats through a government-industry partnership that uses "wargaming" analyses — i.e., virtual techniques to model and assess threats — to evaluate manufacturing cyberthreats and test strategies for ensuring supply-chain cybersecurity. As part of this partnership, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) should implement a pilot program to spread robust and scalable cybersecurity best practices throughout manufacturing-based supply chains. Coordinating the resources and expertise of other federal agencies — including the Nuclear Security Enterprise (NSE), the Department of Defense (DOD) Digital Manufacturing Institute (MxD), the National Institutes of Standards and Technology (NIST) Manufacturing Extension Partnership (MEP), and the DOD Cybersecurity Maturity Model Certification (CMMC) program — with the resources and expertise of external entities (e.g., academic institutions) will enable the administration to become more proactive in anticipating and neutralizing cyberthreats, thus enhancing the stability and security of U.S. manufacturing supply chains.

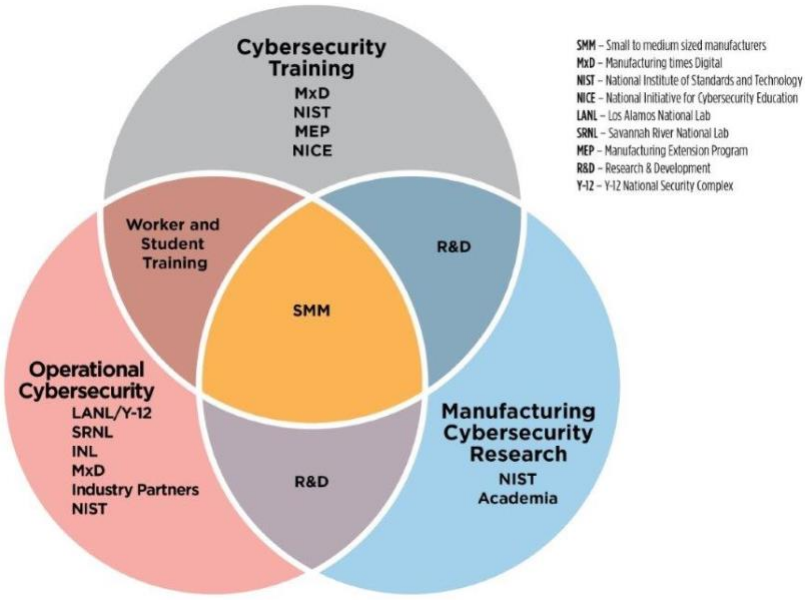
Challenge and Opportunity

Cybersecurity vulnerabilities pose major threats to the U.S. economy, innovation ecosystem, and public safety. The magnitude of these threats demands a commensurate response: one that has not yet manifested. To date, CISA has focused its resources on critical sectors including energy, finance, and healthcare, while largely overlooking manufacturing. Agencies that have paid greater attention to manufacturing — such as DOD and NIST — have been more concerned with best practices and standards compliance than with operational cybersecurity. Fortunately, a shift in perception is occurring. Domestic manufacturing and the defense industrial base are becoming higher priorities in the eyes of policymakers and the public. This creates an opportunity for the Biden-Harris administration to rethink and strengthen the federal approach to manufacturing cybersecurity.

To do so, the administration can build on the existing Supply Chain Cybersecurity Initiative (SCCI), a partnership led by the Los Alamos National Laboratory (LANL) and the Y-12 National Security Complex (Y-12). LANL and Y-12 have a unique perspective on manufacturing and supply-chain security challenges, extensive experience operating and maintaining secure manufacturing enterprises, strong capabilities in large- and small-scale precision manufacturing, and deep expertise in machining and inspection derived from the rigorous requirements of manufacturing and protecting nuclear weapons.

Two primary elements of the SCCI concept are (1) a secure collaboration environment (SCE) for protecting information across the supply chain, and (2) deployment of a manufacturing operations center (MOC) that uses a "wargaming" approach to evaluate and respond to manufacturing cyberthreats: i.e., by continuously modeling supply-chain networks and their dynamic threat environment. These activities extend the DOD's CMMC program and align with the Cyberspace Solarium Commission's recommendation (Recommendation 5.2.1) to focus on sharing and fusing threat information.

SCCI is working with partners from the public, private, and academic sectors to develop foundational technologies required to support the MOC concept. The goal of the MOC is to continually integrate sensor data from SMM networks with relevant threat information in a virtual model of the SMM supply chain. Model outputs improve understanding of manufacturer-specific vulnerabilities to evolving and emerging cyberthreats and inform response strategies. This in turn supports a shift from a reactive to a proactive approach to manufacturing cybersecurity.



The SCCI partnership is a grassroots "coalition of the willing" as illustrated in the figure above, and has already laid much of the foundation for the MOC. Work completed to date includes demonstration of a prototype emulation system for modeling manufacturing networks as well as integration of the emulation system with network sensor technology and a system for incorporating malicious network traffic.

Plan of Action

With capabilities developed to date, the SCCI partnership's MOC is ready to move forward with targeted wargaming activities when funding and support is available. The federal government should allocate the former and should direct CISA, DOD, NIST, and other relevant federal agencies to provide the latter. Applying virtual wargaming technologies to the entire manufacturing supply chain is a challenging task. As such, the federal government should first support a pilot project that tests the capacity of the MOC to model and assess cyberthreats on a subset of SMM companies, such as MxD (Manufacturing times Digital) partnership members. The pilot project should comprise the following activities, to be conducted by the SCCI in partnership with federal agencies listed above as well as academic and other external stakeholders:

Task 1 – Finalize and acquire hardware and software needed to emulate shop-floor control systems.

Task 2 – Develop capabilities to identify anomalous data and securely store these data using a restricted access model and/or database.

Task 3 – Provide SCE needed for enhanced information handling.

Task 4 – Demonstrate capabilities for evaluating manufacturing threats, carrying out wargaming analyses, and proposing threat-remediation approaches.

Task 5 – Define next steps for MOC scale-up.

The pilot project should emphasize the importance of a "classified mindset in an unclassified environment", both among SMM participants and across the project team. SMM networks contain sensitive information that belongs to individual manufacturers as well as to their vendors and customers. DOD's CMMC program is designed to protect this information. However, the current version of CMMC focuses on compliance at a point in time rather than on continuous assessment of the dynamic threat environment as provided by the SCCI wargaming approach.

The CMMC organization supports the SCCI MOC and should be brought on board as an active participant. CMMC could contribute by collecting and providing network information needed for wargaming. The NIST MEP has expressed similar willingness to leverage its national network of agents to contribute to network data collection and provision.

The SCCI MOC's wargaming approach would use the network information collected by partners such as the NIST MEP and the CMMC organization to construct a "representative" model of SMM networks.[1] This emulation will help pinpoint vulnerabilities in manufacturing supply chains and will be a valuable resource for evaluating solutions from different cybersecurity vendors. Because the model will rely on sensitive information, it must be protected with rigorous access controls just as if it were highly classified.

The expected cost of the pilot project is $30 million over a period of three years. The project should be led by the existing SCCI team because of (i) the team's unique experience with operational cybersecurity in a rigorous manufacturing environment; (ii) the foundational progress the team has made (with a diverse set of partners in the public, private and academic sectors) towards virtual wargaming to support manufacturing cybersecurity; and (iii) the team's proven ability to apply a classified mindset to an unclassified environment. Key agencies and programs that would be engaged in planning and operationalizing the project include CISA, the NSE, the MxD partnership, the NIST MEP, and the DOD CMMC program.

Conclusion

The importance of the security and integrity of manufacturing supply chains was demonstrated most recently by the difficulties in responding to the coronavirus (e.g., securing sufficient personal protective equipment). Harms associated with supply-chain failures could be far worse should an adversarial individual or nation state be able to identify critical "pinch points" and weaponize network vulnerabilities. The wargaming system for evaluating manufacturing cyberthreats is designed to accommodate a dynamic threat environment and serve as a key component in the protection of the manufacturing supply chain.

[1] The model contains the key elements of the different networks. To reduce the number of nodes associated with the model, it does not duplicate configurations that are used in multiple applications.

Frequently Asked Questions

1. Aren't all cybersecurity practices proactive? What is different about the wargaming approach to manufacturing threat evaluation?

Most cybersecurity practices are reactive in nature because they address weaponized vulnerabilities and exploits (the "build higher walls and deeper moats" approach). Wargaming includes these elements, but additionally considers non-weaponized vulnerabilities, zero-day exploits, real-time feedback from network sensors, and intelligence community information. In its fullest expression, wargaming is like having elite hackers with access to continuously updated information from the entire supply chain continuously road-test existing cybersecurity systems.

2. How would the MOC support wargaming?

The MOC is designed as a federated secure operations center focused on the operational cybersecurity of the U.S. manufacturing supply chain. The MOC provides the cyber-physical security required to host wargaming operations and protect associated information at appropriate security levels.

3. Would the MOC have access to "intelligence community" information?

Yes. As a federated operations center, the MOC would be able to access information that is not available to the private sector. However, identified vulnerabilities can be integrated into the wargaming activities without disclosing sensitive or classified (e.g., "sources and methods") information.

4. Would the MOC perform remediation activities to address cybersecurity vulnerabilities?

No. This task is generally better left to the private sector. The MOC would provide vulnerability information related to a specific company's network configuration, but it would not create patches, endorse specific vendor products, etc. Public-sector resources such as the NIST MEP and CISA provide resources for topics ranging from general cybersecurity recommendations to incident response assistance.

5. Why should the government get involved in shoring up manufacturing cybersecurity? Can't the private sector do this?

The government is already involved in manufacturing cybersecurity through the Defense Federal Acquisition Regulation Supplement (DFARS; clause 252.204-7012), the DOD CMMC requirements, and other contracting protocols. Further involvement is warranted due to the critical national-security threats that vulnerabilities in manufacturing cybersecurity pose. Cyberattacks can be deployed as weapons of mass destruction, and cyberattacks targeting the manufacturing sector threaten U.S. physical and economic wellbeing. A highly coordinated, national response is required to address this issue. The private sector is a valuable partner in combatting cybersecurity vulnerabilities, but coordination must reside at the federal level due to the national scale of the threat.

6. How can the MOC possibly create a virtual model of the thousands of networks used across the manufacturing supply chain?

The manufacturing supply chain does consist of thousands of networks. However, many networks use very similar combinations of network elements and software systems. The goal of the MOC is to create a representative model that allows the wargaming approach to significantly improve cybersecurity for much of the supply chain. Achieving this does require the model to capture unique network configurations but does not require duplication of configurations that are used in multiple installations. The initial pilot will cover around 50 to 100 SMM networks, with future expansions conducted in stages.

7. What is the function of the network sensors?

The SMM network configuration information is used to define the node elements and interconnections in the virtual model. The network sensors provide real-time information about what is occurring across the supply chain and provide an "early warning" indicator of potential problems.

8. What information would the network sensors collect? Is that information SMM intellectual property (IP)?

The information collected by the network sensors is "traffic flow" data that relates to anomalous activity, such as communications with a "command and control" server associated with a foreign country or a known malicious web site. No SMM IP data would be collected by the traffic-flow sensors.

9. Aren't there already many sources of threat information?

Yes. But the problem, from the SMM standpoint, is that the threat information is overwhelming. Available threat data includes a list of common vulnerabilities and exposures (CVE) that is frequently changed and updated and is often difficult for the supply chain to interpret. SMMs often don't know which warnings apply to their specific situation. By contrast, the wargaming approach identifies specific network attributes and configurations that are at risk of exploitation under particular scenarios. This threat knowledge can be communicated directly and confidentially to individual SMMs as needed.

10. How would the SMM network information be protected?

When the network configuration information is collected, it would be encrypted and a previously generated, encrypted tag (that can only be decoded by a MOC administrator) would be attached. This process would anonymize the information as it is used in the virtual model while maintaining a link that can be used to privately communicate specific vulnerability information to individual companies. In addition, the wargaming activities would be conducted on limited-access, air-gapped servers that would be protected as if they were processing classified information.

11. Could private industry use the wargaming model to test their products?

Industry could work with the MOC to test products such as anomaly-detection sensors or intrusion detectors in the virtual wargaming environment. However, no copies of the representative model will be allowed "out of the MOC."

12. How would the wargaming process affect the CMMC process?

The CMMC process certifies that a company is compliant with graded requirements at a point in time. It does not address the company's ability to deal with cybersecurity issues at a later date, nor does it cover

a company's ability to respond to substantial changes in the threat environment. By contrast, the MOC would continually introduce newly discovered exploits, as well as previously known and potentially weaponized vulnerabilities, into the wargaming process. This advances the CMMC concept to maintain continued relevance and better address the dynamic threat environment.

13. Why should this effort involve the Nuclear Security Enterprise (NSE)?

Since 1945, the NSE has demonstrated exceptional information-security capabilities while producing and maintaining the nation's stockpile of nuclear weapons. This has involved operating a distributed network of design and manufacturing complexes, with international partners, under rigorous manufacturing and operational cybersecurity requirements. While NSE manufacturing-site operations are often highly classified, the cybersecurity challenges are very similar to what is faced by the private sector. The NSE's ability to apply a classified mindset to unclassified operations is a very valuable resource for the U.S. manufacturing supply chain. Another example of the many NSE resources that can be leveraged is the Nuclear Weapons Cyber Assurance Laboratory (NWCAL), which is concerned with issues like malware embedded in a supply chain.

14. How would NWCAL resources support the manufacturing threat evaluation wargaming activities?

NWCAL is LANL's response to threats to the laboratory's national-security mission and weapons programs. NWCAL mitigates risk by providing cyber-physical and technical software assurance for classified manufacturing operations. Lessons learned from this effort are directly applicable to the industrial base as part of the MOC, and are focused on applying a classified mindset to unclassified operations. The major functions of the NWCAL relevant to industry applications are:

- Threat, attack, and incident analysis.
- Hardware, firmware, and software analysis.
- Cyber-physical and operational technology assessments.
- Reverse engineering (hardware, firmware, software, communications).
- Research to advance cybersecurity assurance technologies.

About the Authors

William (Bill) Barkman possesses extensive experience in the precision manufacturing operations required to produce nuclear weapons components. He serves as a program manager for precision-manufacturing activities and is frequently involved in technical consultations with the National Nuclear Security Administration (NNSA) weapons-design laboratories. Bill has been responsible for the development of machining and inspection systems capable of automated operations in rigorous manufacturing environments. He has experience with "non-conventional" metal removal processes such as diamond turning and ceramic grinding, as well as extensive experience in the development and execution of collaborative partnership activities (e.g., NNSA Thrust Areas for Agile Machining and Inspection, Digital Radiography, and Noncontact Inspection; manufacturing and cybersecurity research projects with academia; the public/private Cost Effective Machining of Ceramics program; and the Supply Chain Cybersecurity Initiative). Bill holds seven manufacturing-related patents and has authored over 45 technical publications, including a book titled *In-process Quality Control for Manufacturing* (Marcel Dekker, Inc., 1989). He produced a short course on manufacturing variability.

Rich Taylor is an R&D Manager for the Weapons Research Services, Secure Networks and Assurance group (WRS-SNA) at Los Alamos National Laboratory (LANL), as well as Director for the LANL Nuclear Weapons Cyber Assurance Laboratory (NWCAL). The WRS-SNA group combines related disciplines in IT operations, network security, and software engineering with a goal of encouraging a security-focused development operations culture to support programs across the LANL weapons-production organization. The NWCAL is a new, pioneering initiative at LANL responding to threats to the laboratory's national-security mission and weapons programs. NWCAL mitigates mission risk by providing cyber-physical and technical software assurance. Leveraging this capability in supply-chain risk assessments helps bolster understanding of both cyber and physical risks to our nation's critical supply chains. Rich has been involved in cybersecurity since 2001. Much of his earlier work focused on vulnerabilities of specialized information systems such as banking networks, VoIP systems, and other proprietary systems. His later work focused on supply-chain vulnerabilities with an emphasis on small- to medium-sized manufacturers. Rich currently focuses on cybersecurity vulnerabilities in nuclear weapons production, including the supply chain, cyber-physical systems on manufacturing floors, and critical data associated with weapons production. Rich also serves as the Operational Technology co-chair of the Nuclear Enterprise Assurance Digital Systems Assurance Working Group (NDSAWG).

Dennis Miller is senior technical advisor for manufacturing and manufacturing-related activities (e.g., technology development, cybersecurity, and engineering services) conducted by the Y-12 National Security Complex in Oak Ridge, TN. In this role, Dennis leads national security-significant programs for government and industry. He leverages both the Pantex nuclear weapons assembly plant in Amarillo, TX and Y-12's core capabilities to address customers' needs, proposing solutions for difficult technical national-security challenges. Miller leads key initiatives to ensure the cybersecurity of the manufacturing industrial base: the supply chain of small- to medium-sized manufacturers critical to the nation's economy and national defense.

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans, and readying them for Day One of the next presidential term. For more about the Day One Project, visit **dayoneproject.org**.

The Day One Project offers a platform for ideas that represent a broad range of perspectives across S&T disciplines. The views and opinions expressed in this proposal are those of the author(s) and do not reflect the views and opinions of the Day One Project or its S&T Leadership Council.