Stanley Center
FOR PEACE AND SECURITY

ANALYSIS & NEW INSIGHTS

An Internet of Nuclear Things

Emerging Technology and the Future of Supply Chain Security

By Wyatt Hoffman & Tristan A. Volpe

Emerging technologies enabled by digitization—notably additive manufacturing—are alluring for the nuclear industry as it works to lower financial costs and remedy quality-control concerns with aged production lines. While cyberphysical manufacturing technology could increase the efficiency and visibility of supply-chain operations, the digital nature of this technology introduces new threats. To be sure, there are several ways to manage these risks as some version of an Internet of Nuclear Things emerges over the next decade. The key is for industry to take a proactive approach by building these remedies into the technology and policy of supply chain security.

Introduction

The current state of affairs for the civil nuclear industry is bleak. Nuclear energy faces economic challenges from cheap natural gas and renewable sources of electricity. Geopolitical factors are intensifying the competition for global market share among private and state-owned enterprises. At the same time, the nuclear sector is beset by burgeoning reactor construction costs and concerns about supply chain integrity.[1]

Over the last five years, financial overruns stalled work on several new reactor projects, most notably the Vogtle project in Georgia that drove the venerable Westinghouse Electric Company into bankruptcy.[2] Quality control issues plagued reactor manufacturers in Russia, China, and even South Korea and the United States.[3] In two cases, government regulators found evidence of American and South Korean vendors introducing flawed components into the nuclear supply chain by mistake, while others faked safety and certification tests on substandard parts, thereby delaying build projects or shutting down operational reactors until legitimate components could be swapped in.[4]

Key actors from the nuclear industry—from General Electric Hitachi to Rosatom and the Chinese National Nuclear Corporation—started to invest in emerging technologies to deal with these production problems.[5] Most notably, additive

manufacturing (AM) offered a new means of production that combined innovations in robotics, computational power, and network connectivity to fabricate sophisticated components from digital files. As aerospace and defense firms integrated AM into the industrial base for jet engines, missiles, and satellites, nuclear energy programs followed suit by exploring whether the technology could improve reactor construction, perhaps "by enhancing the flexibility and adaptability of production lines."[6] Research and development efforts experimented with AM techniques for fabricating metallic reactor components with "new complex designs," including nuclear fuel rod assemblies and large pressure vessel cylinders.[7] Moreover, the digital nature of AM technology promised to "reshape the very nature of supply chains," by enabling companies to shrink or even eliminate the traditional web of subcontractors and global logistics.[8]

The maturation of AM in the years ahead is likely to accelerate the broader trend toward digitization of manufacturing processes and supply chains, including the diffusion of sensors and devices in an industrial Internet of Things. Embracing these technologies could improve the economic position of struggling nuclear firms. The ultimate goal is to develop the capacity to fabricate a wide range of certified nuclear components on demand, without having to extensively retool production lines or interpret designs. Indeed, many firms are leveraging the digital connectivity built into AM and other modern production technologies to enhance the efficiency of supply chains and address more fundamental quality-control problems. As a result, these innovations could lay the foundation for the emergence of an Internet of Nuclear Things (IoNT), an interconnected ecosystem of devices and machines spreading throughout production lines for nuclear energy projects.[9]

On initial consideration, an IoNT appears to offer promising solutions to the current challenges facing nuclear industry. Yet these technologies could introduce a new range of cyber risks, including threats to the confidentiality, integrity, and availability of data and fabricated physical components in an IoNT. We find that there are numerous technical options being developed to manage these cyber risks, many suitable for nuclear vendors. But it cannot be assumed that all manufacturers will head down a path toward effective risk management in this new digital ecosystem. If geopolitical and economic trends continue to constrain the nuclear industry, some vendors may end up rushing to adopt an IoNT without due consideration of the intrinsic vulnerabilities and vectors for malicious attack. Thus, the industry may be approaching a juncture that will shape the future of safety and security practices for the manufacture of civil nuclear technology.

Nuclear Supply in the Digital Age

As disruptive technologies for manufacturing processes and supply chains continue to gain momentum, the nuclear industry is unlikely to remain insulated from these transformations.[10]

The future of the manufacturing sector lies at the intersection of cyber-physical manufacturing capabilities, digital connectivity, and the constant collection and analysis of massive amounts of data, trends encapsulated in such concepts as "Industry 4.0" and GE's "Brilliant Manufacturing."[11] Nuclear firms are already developing and adopting some of the technologies that could form the foundation for an IoNT to emerge over the next decade. A brief review of AM illustrates the general benefits of combining the cyber and physical domains for nuclear production lines.

AM technology is alluring for the nuclear industry because it offers the promise of an agile, cost-effective means of production, especially as nuclear-capable supply chains atrophy in the United States and parts of Europe. Small batches of mission-critical reactor components, for instance, can be difficult and expensive to source if they are produced using traditional methods, as producers often need long lead times to establish processes for forging and casting parts.[12] AM offers a more agile way to fabricate components with geometries and characteristics simply not possible before with subtractive machine tools, often at a fraction of the cost of traditional production lines. The potential cost savings come from utilizing recent innovations in robotics, computation, and digital networks to fabricate physical components from digital build files. These virtual blueprints contain the design information needed to produce a desired component along with commands that guide the automated build process itself.

Whereas traditional manufacturing requires skilled machinists to configure and retool each production line, the ultimate goal of cyber-physical manufacturing is to capture this tacit knowledge in the digital realm, where it can be automated and saved, thereby allowing fully certified parts to be printed on demand. For instance, research and development efforts are under way to use the data from remote sensors in metallic AM platforms to provide instant feedback on the quality and integrity of the component being built; the ultimate goal is to certify components for aerospace or nuclear applications in real time during the fabrication process.[13] Instead of sinking high costs into traditional nuclear production lines that atrophy during periods of low demand, additive manufacturing offers the nuclear industry the promise of eventually being able to print certified components whenever needed from digital build files.

This family of technologies for physical production and digital integration all rely on the continuous creation, collection, and analysis of data. The design of the component takes the form of a digital blueprint, translated into multiple formats used to communicate with devices for fabrication. Tacit knowledge of production processes and other forms of proprietary information are captured in the digitized instructions. Additional information is derived from the production process and through various side channels. Finally, metadata is created throughout manufacturing and operations. In short, the impact of these technologies is in not simply the digitization of information but in generating a range of entirely new sources of data that can be harnessed toward improving processes and products. Machines and devices

throughout a production process, and even the products themselves, are being linked in webs that encompass large segments of supply chains. With such a network, manufacturers and operators can apply data analytics and machine learning to harness the information collected from this web of devices to increase efficiency and performance.

General Electric provides a clear example of the opportunities created by networked production technology such as additive manufacturing. GE used the new production technology to retrofit jet engines with special sensor housings that can transmit real-time data on engine performance in-flight.[14] The company's newest jet engine will be produced with more than a third of 3-D printed components. Moreover, each new engine will have a unique "digital twin" generated during production; the sensors built into the engine will send data during performance back to the digital twin, where it will be analyzed to "help operators predict the right time for maintenance and keep the plane in the air more."[15]

The same innovations are being applied to nuclear technology. For instance, GE's Digital Power Plant incorporates digital twins of nuclear assets that are remotely monitored to improve performance and maintenance.[16] Its Predix software is a cloud-based platform that collects data from power plants and remotely analyzes it to assist in the management of operations. The software harnesses "enterprise data visibility" to increase efficiency by minimizing outages and adopt a predictive rather than reactive approach to maintenance.[17] In 2016, GE made a deal for its "first and largest IoT (internet of things) enterprise-wide deployment" of Predix software for managing Exelon's power plants in 48 US states.[18] Naturally, other companies are innovating in this space. IBM and Siemens' collaboration on the "Smart Factory" concept seeks to incorporate sensors, IoT, and cognitive computing for complex challenges like maintenance of rotating machinery.[19]

While in the nuclear context current applications have been limited mainly to managing plant operations, these kinds of platforms could grow to incorporate aspects of production throughout the supply chain. The generation of a digital twin for a given component creates a "digital thread"—a "single, seamless strand of data" stretching from design through production and into performance monitoring, maintenance, and ultimately disposal. The integration of multiple threads from parallel processes into a "digital tapestry" takes the potential to leverage data one step further.[20] In addition to spreading vertically throughout production and operation of components for nuclear power plants, these capabilities could extend across the range of nuclear fuel cycle activities.

Thus, the fusion of these capabilities—cyberphysical manufacturing, digital connectivity, network integration, and data analysis—in an IoNT creates the potential for not just incremental improvements but radical changes in nuclear supply chains and operations. There is no predetermined framework for what this system would look like, as layers of technology could be interwoven organically (in a manner similar to how the Internet of Things in general has evolved). An IoNT could entail a range of potential digital ecosystems—from merely the devices connected to a single production process to an elaborate network spanning a supply chain and operations.

Cyber Risk in an Internet of Nuclear Things

The prospect for an IoNT to emerge raises questions about how the digital nature of the technology might increase cybersecurity threats to nuclear industry. With the proliferation of digital connections and devices comes an inevitable expansion of the cyberattack surface. This has been the case for the manufacturing sector more broadly, which has been targeted with increasingly frequent and costly cyberattacks.[21] The massive WannaCry and NotPetya ransomware attacks in 2017 demonstrated the potential for cyberattacks to rapidly spread and cause severe disruption for manufacturers.[22] Cyber vulnerabilities, including throughout supply chains, are already an escalating concern for the nuclear industry.[23] An IoNT could not only increase these vulnerabilities but expand the potential impacts of cyberattacks by creating opportunities to steal sensitive information and even cause damage in the physical world.

This concern is heightened by the integration of information technology (IT) and operational technology (OT) within an industrial Internet of Things, which potentially exposes critical systems that are designed and oriented toward an entirely different set of risks and priorities to cyberattacks. These include industrial control systems crucial to the safe operations of an industrial process. IT and OT generally differ in their technical standards and priorities.[24] For instance, the imperatives of OT are safety, reliability, and minimizing downtime, which can each militate against the frequent updating and patching typical of IT. Legacy systems in particular tend to be patched and updated far less frequently than IT systems and are in service for far longer. Connecting insecure OT systems with Internet-connected devices thus potentially opens new avenues for cyberattacks to create physical effects through the machines they operate.

Emerging and evolving cyber-physical manufacturing processes may exacerbate these risks by increasing the potential scope and scale of cyberattacks targeting physical fabrication processes. For instance, each stage in a typical AM process presents attractive targets for cyberattacks — including the initial digital build files and subsequent files created for use by 3-D printers (typically a .STL file) or to guide robotic printer components.[25] The confidentiality of design files and other proprietary information such as printer specifications could be compromised, for instance, if a malicious actor intercepts communication between devices. A cyberattack could target the printer operations itself by, for example, shutting down cooling fans to cause it to overheat, thus reducing availability and disrupting production. A toolpath file could be manipulated to set the printer off course, ruining the product or even causing the machine to break the tool.[26]

The greatest concern for safety would be a cyberattack targeting the integrity of critical data. The most insidious form of attack could alter a digital blueprint or .STL file to insert an internal "void" into a design at a point where it could undermine structural integrity and cause the component to malfunction or even break down during use. This would take one of the chief advantages of AM—the ability to manipulate the internal structure of a product—and turn it against the manufacturer.

A void attack could go undetected by standard quality-control processes, especially if the malicious actor compromised the integrity of these inspection methods. To be sure, the sophistication of such an operation would require an in-depth understanding of the quality-control mechanisms and product specifications, not to mention the ability to overcome cyber-defenses without being detected. However, the possibility of these attacks is not remote, especially since researchers are experimenting with techniques to more readily place voids in .STL files.[27] In a prime example from 2016, a university research team introduced malicious code into digital build files to "sabotage the 3-D printed propeller of a quadcopter [unmanned aerial vehicle], causing the quadcopter to literally fall from the sky."[28] If this sort of operation was directed against supply chains used by nuclear industry, the results could be problematic, to say the least.

In sum, AM and cyber-physical capabilities more broadly promise to make cybersecurity more difficult for the manufacturing sector. A publication by the National Institute of Standards and Technology following a symposium on digital manufacturing called cybersecurity threats the "Achilles heel of the current manufacturing revolution."[29] In the context of nuclear industry, however, these business risks become matters of public safety and international security.

From Vulnerability to Resilience: Securing the Nuclear Supply Chain

If left unchecked, the vulnerabilities created by the steady trend toward digitization and interconnection could result in unacceptable cyber risks, ranging from the loss of sensitive proprietary information to the spread of compromised components throughout nuclear infrastructure. But these risks are not intractable. The same information visibility within an IoNT that would create opportunities for cyberattacks could be harnessed by a range of novel innovations, not only to counter immediate cyber threats but to achieve greater oversight of complex and globally dispersed supply chains. Such innovations are being explored by a range of industries and researchers for the shared challenges of cyber supply chain risk management, and nuclear industry can benefit from these common solutions.

At the level of generic additive manufacturing processes, a variety of methods and approaches are being developed to ensure the integrity of products against potential flaws and malicious interventions. These include techniques for in situ monitoring of fabrication combined with machine learning and high-performance computing. For instance, researchers are developing techniques for verification using acoustic monitoring of a 3-D printer during fabrication; the sounds produced by a printer comprise an audio signature that computer algorithms can assess against a reference model of the "correct" audio recording for the given component.[30]

Beyond a single fabrication process, manufacturers need to be able to track and authenticate materials and products throughout each stage in increasingly complex webs of production. Toward this end, new and existing technologies and practices allow for traceability of materials and products throughout the supply chain, such as the use of radio frequency identification or chemical tags.[31] The ability to embed sensors into manufactured components to monitor performance provides further opportunities to safeguard against tampering.

The same principle can be applied to digital files such as sensitive designs, which can be tracked and authenticated via digital signatures and access to which can be controlled through limiting authorization via licensing keys.[32] Hardware can similarly be traced through digital controls. An illustrative example of the integration of these features is Intel's "Transparent Supply Chain" concept, which aims to provide "near real-time transparency into a part's provenance" by storing encrypted information related to each product's origin in a special module attached to the product.[33] This allows Intel to verify that the hardware and firmware have not been tampered with before reaching the end user.

Moreover, technologies with even greater potential to transform supply chains are maturing, including blockchain. Most commonly associated with cryptocurrencies like Bitcoin, blockchain is a method for recording information related to transactions in a "distributed ledger"[34] that does not rely on any single secure data repository. Such an "immutable" ledger could record transactions, transfers of materials, and production processes between specific nodes or throughout a supply chain. For example, the output of a set of 3-D printers could be continuously recorded in a blockchain with varying levels of detail, accessible by a limited number of relevant actors. The technical and practical challenges to implementation of this nascent technology should not be underestimated, but proofs of concept are already being developed for aerospace and defense industries.[35]

Taken together, these innovations comprise a somewhat counterintuitive approach to cybersecurity: rather than trying to hide or isolate vulnerable data—such as through air-gapping systems by disconnecting them from the Internet—such innovations harness information visibility to cross-reference and verify different sources of data and create feedback loops that prevent, detect, or minimize the impacts of accidental malfunction or malicious attack. The air-gapping approach has been proven to be an insufficient guarantor of security by Stuxnet and other cyberattacks. In contrast, cutting-edge approaches to supply chain security for information and communications technologies strive for

transparency and traceability.[36] While some of the innovations described here are nascent and have yet to be proven, they offer a more promising approach to managing the risks of digitization in the nuclear industry.

The Future of Risk and Innovation in Nuclear Industry

An IoNT would entail tradeoffs between liabilities and opportunities for supply chain security. In some cases, this risk calculus with respect to specific technologies will be apparent. For instance, the information gleaned from side-channel monitoring of 3-D printers could verify the integrity of a fabrication process or, conversely, be harnessed by attackers to steal design information.[37] But in many cases it may be hard to anticipate how malicious actors will exploit technologies.

The net impact of an IoNT architecture on the overall risk landscape for the nuclear industry will be difficult to assess, as it depends on how these technologies are designed and adopted in specific contexts. This presents an uncertain future for the nuclear industry if an IoNT emerges and evolves. The industry may end up unintentionally increasing these risks if cyber-physical manufacturing capabilities are adopted in an ad hoc manner, in the absence of common security standards, and with little attention to the potential attack vectors being created.

However, a proactive approach to building security into an IoNT could enhance vendors' oversight of materials, processes, and products. It could also improve their ability to detect and address any anomalies throughout the supply chain and prevent malicious interventions. While individual companies and countries will vary in their approaches to these technologies, all actors face incentives to ensure supply chain security; the protection of intellectual property and confidence in the integrity and reliability of products is crucial to the commercial viability of nuclear energy.

The challenge is that geopolitical factors shape the incentive structure for nuclear industry and may steer it toward one trajectory over the other. Western nuclear vendors are either declaring bankruptcy or losing global market share.[38] Russia and China are quickly becoming the dominant nuclear suppliers because they leverage "nuclear trade to build political relations and acquire leverage over key countries."[39] Unfortunately, the use of nuclear exports as a tool of grand strategy often leads Moscow and Beijing to "turn a blind eye to lax nuclear industry standards and weak nonproliferation assurances in recipient countries."[40] These factors combine to create a risk-acceptant incentive structure for many companies, especially vendors in the West and East Asia struggling to compete with Russian and Chinese state-owned nuclear enterprises.[41] In this context, the emergence of technologies that are attractive from an economic perspective but entail unclear risks is concerning, as it cannot be assumed that digital supply chain security will always be a paramount consideration.

Toward a Proactive Approach to an Internet of Nuclear Things

This early period in the emergence of an IoNT presents an opportunity to shape its growth along a more positive path. The purpose of scoping out the cyber risks alongside the innovations for ensuring safety and security is to demonstrate how these technologies could lead to a number of different outcomes. In particular, the private sector will shape this future risk landscape through the pathways of technological development. A proactive approach is needed by like-minded stakeholders in the policy community to ensure the conditions for safety and security in an IoNT. Any approach will need to be flexible as these technologies evolve and the risks become clear. But we can begin here by offering a few recommendations for the contours of such an approach:

First, determine the requirements for ensuring the integrity of processes and products in the context of an IoNT. This entails taking stock of the risks facing the nuclear industry with respect to the specific technologies adopted and exploring the range of mitigation measures. For instance, with respect to additive manufacturing in particular, this may include traceability of the material feedstock, in situ production monitoring, quality-control tests, tracking mechanisms for finished products, encryption of data flows at each step in the chain, cybersecurity of individual devices, and adequate training of personnel.

Fortunately, efforts to determine such requirements are already under way, including most notably at the National Institute of Standards and Technology, which has initiatives on cyberphysical manufacturing and supply chain risk management in the context of information and communications technologies.[42] This would aid with the identification of specific capabilities that would help provide assurance, such as some of the innovations discussed here. Of course, the focus of this discussion on novel innovations is not to downplay the essential role of proven measures to ensure cybersecurity, such as basic cybersecurity training for personnel. These various elements should be incorporated in a broader approach to security in the context of an IoNT.

Second, translate these requirements into standards for nuclear industry. Numerous efforts are also being pursued to develop technical standards across the range of technologies that could comprise an IoNT, most notably the Additive Manufacturing Development Structure initiative for developing AM standards founded by the International Standards Organization (ISO) and the American Society for Testing and Materials (ASTM).[43] The nuclear industry can build on this foundation and follow others, such as aerospace, that are leading in the development of additive manufacturing processes for critical applications. The Federal Aviation Administration has already certified 3-D printed parts for in-flight use and is developing an Additive Manufacturing Strategic Roadmap to provide guidance to industry, including on part and process certification.[44]

Standards for the certification of nuclear components could incorporate specific mechanisms and innovations discussed above to verify the integrity of products, perhaps in ways that are superior to traditional quality-control methods. These standards for certification would help differentiate suppliers working to ensure the integrity of supply chain operations from those failing to do so; international recognition of a single standard could go a long way toward harmonizing various national regulatory approaches to the civil nuclear industry.

Finally, internationalize the implementation of such standards and foster broader norms relating to the nuclear industry's adoption of these capabilities. At the level of private sector and civil society, governments should collaborate with companies, universities, and other institutions in the development of technologies feeding into an IoNT toward the development of secure technology and mutually beneficial norms. At the national level, export controls could incorporate specific provisions to ensure vendor oversight of dual-use cyber-physical manufacturing capabilities exported abroad. The International Atomic Energy Agency already provides guidance on cybersecurity of nuclear facilities, and this could expand to address specific supply chain concerns.

The dilemmas of an IoNT will be a complex balancing act—not just between the benefits and risks of digitization but between different kinds of risk intrinsic to the design of this ecosystem. The problem is not a lack of technical solutions for cybersecurity; rather it will be difficult to align incentives within the global nuclear order to realize such goals. The greatest concern is the intersection of these emerging technologies with a devolving nuclear order that creates incentives for industry to adopt an IoNT architecture with safety and security as an afterthought. But at this early stage of development, a proactive approach can head off these cyber risks while leveraging an IoNT to ensure the integrity of critical nuclear infrastructure and the security of sensitive information.[45]

Endnotes

[1] Jessica R. Lovering, Arthur Yip, and Ted Nordhaus, "Historical Construction Costs of Global Nuclear Power Reactors," *Energy Policy* 91 (April 1, 2016): 371–82, https://doi.org/10.1016/j.enpol.2016.01.011; "The U.S. Nuclear Energy Enterprise: A Key National Security Enabler," Energy Futures Initiative, August 2017, https://static1.squarespace.com/static/58ec123cb3db2bd94e057628/t/59947949f43b55af66b0684b/1502902604749/EFI+nuclear+paper+17+Aug+2017.pdf.

[2] Diane Cardwell and Jonathan Soble, "Westinghouse Files for Bankruptcy, in Blow to Nuclear Power," *New York Times*, March 29, 2017, https://www.nytimes.com/2017/03/29/business/westinghouse-toshiba-nuclear-bankruptcy.html.

[3] Emma Lecavalier, "Russian Nuclear Power: Convenience at What Cost?," *Bulletin of the Atomic Scientists*, \ October 16, 2015, https://thebulletin.org/russian-nuclear-power-convenience-what-cost8809; "China Nuclear Reactor Delayed Again on 'Safety Concerns': China Daily," *Reuters*, February 13, 2018, https://www.reuters.com/article/us-china-nuclear/china-nuclear-reactor-delayed-again-on-safety-concerns-china-daily-idUSKBN1FX02P.

[4] Choe Sang-Hun, "Scandal in South Korea Over Nuclear Revelations," New York Times, August 3, 2013, https://www.nytimes.com/2013/08/04/world/asia/scandal-in-south-korea-over-nuclear-revelations.html; "How Two Cutting Edge U.S. Nuclear Projects Bankrupted Westinghouse," Reuters, May 2, 2017, https://www.reuters.com/article/us-toshiba-accounting-westinghouse-nucle/how-two-cutting-edge-u-s-nuclear-projects-bankrupted-westinghouse-idUSKBN17Y0CQ.

[5] Office of Nuclear Energy, "Neet-Advanced Methods for Manufacturing Award Summaries," US Department of Energy, May 2016; General Electric, "GE Hitachi Selected to Lead U.S. Department of Energy Advanced Nuclear Technology Research Project," press release, June 2016; Clare Scott, "ROSATOM Announces New Additive Manufacturing Subsidiary," 3DPrint.com, February 13, 2018, https://3dprint.com/203531/rosatom-am-subsidiary/.

[6] Shawn Brimley, Ben FitzGerald, and Kelley Sayler, "Disruptive Technology and U.S. Defense Strategy," Disruptive Defense Papers, Center for New American Security, September 2013, 14.

[7] Zeses Karoutas, "3D Printing of Components and Coating Applications at Westinghouse," MIT Workshop on New Cross-Cutting Technologies for Nuclear Power Plants, January 30, 2017. See also "Chinese Experts Unveil First 3D Printed Nuclear Fuel Element," 3ders.org, January 14, 2016, http://www.3ders.org/articles/20160114-chinese-first-3d-printed-nuclear-fuel-element-could-be-widely-used-in-10-years.html; "GE Hitachi, ARC to License Joint Reactor in Canada; Siemens Installs First Live 3D-Printed Part," *Nuclear Energy Insider*, March 21, 2017, https://analysis.nuclearenergyinsider.com/ge-hitachi-arc-license-joint-reactor-canada-siemens-installs-first-live-3d-printed-part; "Westinghouse to Install First 3D-Printed Reactor Fuel Part in 2018," *Nuclear Energy Insider*, November 1, 2017, https://analysis.nuclearenergyinsider.com/westinghouse-install-first-3d-printed-reactor-fuel-part-2018.

[8] Ian Stewart, Dominic Williams, and Nick Gillard, "Examining Intangible Technology Controls—Part 2: Case Studies," Project Alpha, King's College London, June 2016, p. 18, https://projectalpha.eu/examining-intangible-controls/.

[9] Wyatt Hoffman and Tristan A. Volpe, "Internet of Nuclear Things: Managing the Proliferation Risks of 3-D Printing Technology," *Bulletin of the Atomic Scientists*, Vol. 74, No. 2 (March 4, 2018): 102–13, https://doi.org/10.1080/00963402.2018.1436811v

[10] David Livingstone, Caroline Baylon, and Roger Brunt, "Cyber Security at Civil Nuclear Facilities: Understanding the Risks," Chatham House, October 5, 2015, https://www.chathamhouse.org//node/18747.

[11] See Bernard Marr, "Why Everyone Must Get Ready for the 4th Industrial Revolution," *Forbes*, April 5, 2016, https://www.forbes.com/sites/bernardmarr/2016/04/05/why-everyone-must-get-ready-for-4th-industrial-revolution/#7c69f4243f90; General Electric, "GE Launches Brilliant Manufacturing Suite to Help Manufacturers Increase Production Efficiency, Execution and Optimization Through Advanced Analytics," press release, Sept. 29, 2015, https://www.ge.com/digital/press-releases/ge-launches-brilliant-manufacturing-suite.

[12] "U.S. Nuclear Energy Enterprise."

[13] See for example the Accelerated Certification of Additively Manufactured Metals Project at Lawrence Livermore National Laboratory, https://acamm.llnl.gov/about.

[14] Tomas Kellner, "The FAA Cleared the First 3D Printed Part to Fly in a Commercial Jet Engine from GE," *GE Reports*, April 14, 2015. https://www.ge.com/reports/post/116402870270/the-faa-cleared-the-first-3d-printed-part-to-fly-2/.

[15] Yari M. Bovalino and Dmitry Sheynin, "A Treat for the AvGeeks: An Inside Look at GE's 3D-Printed Aircraft Engine," *GE Reports*, July 24, 2017, https://www.ge.com/reports/treat-avgeeks-inside-look-ges-3d-printed-aircraft-engine/.

[16] "Digitisation Experts Explain Benefits for Nuclear," World Nuclear News, July 5, 2017, http://www.world-nuclear-news.org/C-Digitisation-experts-explain-benefits-for-nuclear-05071701.html.

[17] Eric Mino, "Industrial Internet Applications," *Nuclear Plant Journal*, Vol. 34, No. 1, January–February 2016, pp. 20–21, https://nuclear.gepower.com/turnpage.

[18] Alwyn Scott, "GE Signs Exelon in its Largest Power-Plant Software Deal," Reuters, November 15, 2016, https://www.reuters.com/article/us-general-electric-exelon-power/ge-signs-exelon-in-its-largest-power-plant-software-deal-idUSKBN13A1ZF.

[19] "Digitisation Experts Explain Benefits."

[20] Mark Cotteleer, Stuart Trouton, and Ed Dobner, "3D Opportunity and the Digital Thread: Additive Manufacturing Ties It All Together," Deloitte Insights, March 3, 2016, https://www2.deloitte.com/content/dam/insights/us/articles/3d-printing-digital-thread-in-manufacturing/ER_3060-3D-opp-_Digital-Thread_MASTER-1.pdf.

[21] Rutrell Yasin, "Manufacturers Suffer Increase in Cyberattacks," *Dark Reading*, April 20, 2016, https://www.darkreading.com/vulnerabilities---threats/manufacturers-suffer-increase-in-cyberattacks/d/d-id/1325209?.

[22] Sridhar Kota, "A Plan for Defending US Manufacturers from Cyberattacks," *The Hill*, October 20, 2017, http://thehill.com/opinion/cybersecurity/356377-a-plan-for-defending-us-manufacturers-from-cyberattacks.

[23] Sean Lyngaas, "Nuclear Power Plants Have a 'Blind Spot' for Hackers. Here's How to Fix That," Motherboard, April 27, 2018, https://motherboard.vice.com/en_us/article/mbxy33/cyberattacks-nuclear-supply-chain.

[24] See "Cybersecurity for Manufacturing Networks," NDIA Cybersecurity for Advanced Manufacturing Joint Working Group, October 2017, http://www.ndia.org/-/media/sites/ndia/divisions/working-groups/cfam/ndia-cfam-2017-white-paper-20171023.ashx?la=en.

[25] L.D. Sturm, C.B. Williams, J.A. Camelio, J. White, and R. Parker, "Cyber-Physical Vulnerabilities in Additive Manufacturing Systems: A Case Study Attack on the .STL File With Human Subjects," *Journal of Manufacturing Systems*, Vol. 44, No. 1 (2017): 154–164, https://doi.org/10.1016/j.jmsy.2017.05.007.

[26] C. Paulsen, ed., "Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium," April 2015, National Institute of Standards and Technology, US Department of Commerce, doi:10.6028/NIST.IR.8041.

[27] Ibid.

[28] Sofia Belikovetsky, Mark Yampolskiy, Jinghui Toh, Yuval Elovici, "dr0wned—Cyber-Physical Attack With Additive Manufacturing," arXiv:1609.00133, September 1, 2016, https://arxiv.org/abs/1609.00133.

[29] Paulsen, "Proceedings."

[30] Christian Bayens, Tuan Le, Luis Garcia, Raheem Beyah, Medhi Javanmard and Saman Zonouz, "See No Evil, Hear No Evil, Feel No Evil, Print No Evil? Malicious Fill Pattern Detection in Additive Manufacturing," 26th USENIX Security Symposium, August 2017, https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-bayens.pdf.

[31] John Brown, John Ezzard, Simon Goldenberg, and Jeff Haid, "3D Opportunity and Cyber Risk Management: Additive Manufacturing Secures the Thread," Deloitte Insights, August 23, 2016, https://www2.deloitte.com/insights/us/en/focus/3d-opportunity/3d-printing-cyber-risk-management.html.

[32] Ibid.

[33] National Institute of Standards and Technology (NIST), US Department of Commerce, "Best Practices in Cyber Supply Chain Risk Management: Intel Corporation: Managing Risk End-to-End in Intel's Supply Chain," https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Intel_100715.pdf.

[34] For a thorough introduction to blockchain. technology, see Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone, "Blockchain Technology Overview," National Institute of Standards and Technology, 2018, https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf.

[35] Craig Gottlieb, "Blockchain in Aerospace and Defense," Accenture, 2017, https://www.accenture.com/t20170928T023222Z__w__/us-en/_acnmedia/PDF-61/Accenture-Blockchain-For-Aerospace-Defense-PoV-v2.pdf.

[36] NIST, *Best Practices*.

[37] See Mohammad Abdullah Al Faruque, Sujit Rokka Chhetri, Sina Faezi, and Arquimedes Canedo, "Forensics of Thermal Side-Channel in Additive Manufacturing Systems," Center for Embedded and Cyber-Physical Systems, January 15, 2016, https://pdfs.semanticscholar.org/c8ca/d6066871137ecca3003d35b6111ea4107ba2.pdf.

[38] Daniel B. Poneman, "The Case for American Nuclear Leadership," *Bulletin of the Atomic Scientists*, Vol. 73, No. 1, January 2, 2017, pp. 44–47, https://www.tandfonline.com/doi/full/10.1080/00963402.2016.1264211.

[39] Nicholas L. Miller and Tristan A. Volpe, "Geostrategic Nuclear Exports: The Competition for Influence in Saudi Arabia," War on the Rocks, February 7, 2018, https://warontherocks.com/2018/02/geostrategic-nuclear-exports-competition-influence-saudi-arabia/.

[40] Ibid.

[41] Ariel Levite and Toby Dalton, "Leveling Up the Nuclear Trade Playing Field," Carnegie Endowment for International Peace, September 7, 2017, http://carnegieendowment.org/2017/09/07/leveling-up-nuclear-trade-playing-field-pub-73038; Mark Hibbs, "Does the U.S. Nuclear Industry Have a Future?," Carnegie Endowment for International Peace, accessed January 23, 2018, http://carnegieendowment.org/2017/08/10/does-u.s.-nuclear-industry-have-future-pub-72797.

[42] Paulsen, "Proceedings."

[43] Clare Naden, "ISO and ASTM International Unveil Framework for Creating Global Additive Manufacturing Standards," International Organization for Standardization, October 7, 2016, https://www.iso.org/news/2016/10/Ref2124.html.

[44] Beau Jackson, "FAA to Launch Eight-Year Additive Manufacturing Road Map," *3D Printing Industry*, October 2017, https://3dprintingindustry.com/news/faa-launch-eight-year-additive-manufacturing-road-map-123108/.

[45] For an assessment of how the digital nature of AM technology could be flipped from a liability into an asset for nuclear nonproliferation, see Hoffman and Volpe, "Internet of Nuclear Things."

About the Author

Wyatt Hoffman is a research analyst with the Cyber Policy Initiative at the Carnegie Endowment for International Peace.

Tristan A. Volpe is an assistant professor in the Defense Analysis Department at the Naval Postgraduate School and a nonresident fellow at the Carnegie Endowment for International Peace.

About Us

The Stanley Center for Peace and Security partners with people, organizations, and the greater global community to drive policy progress in three issue areas—mitigating climate change, avoiding the use of nuclear weapons, and preventing mass violence and atrocities. The center was created in 1956 and maintains its independence while developing forums for diverse perspectives and ideas. To learn more about our recent publications and upcoming events, please visit stanleycenter.org.