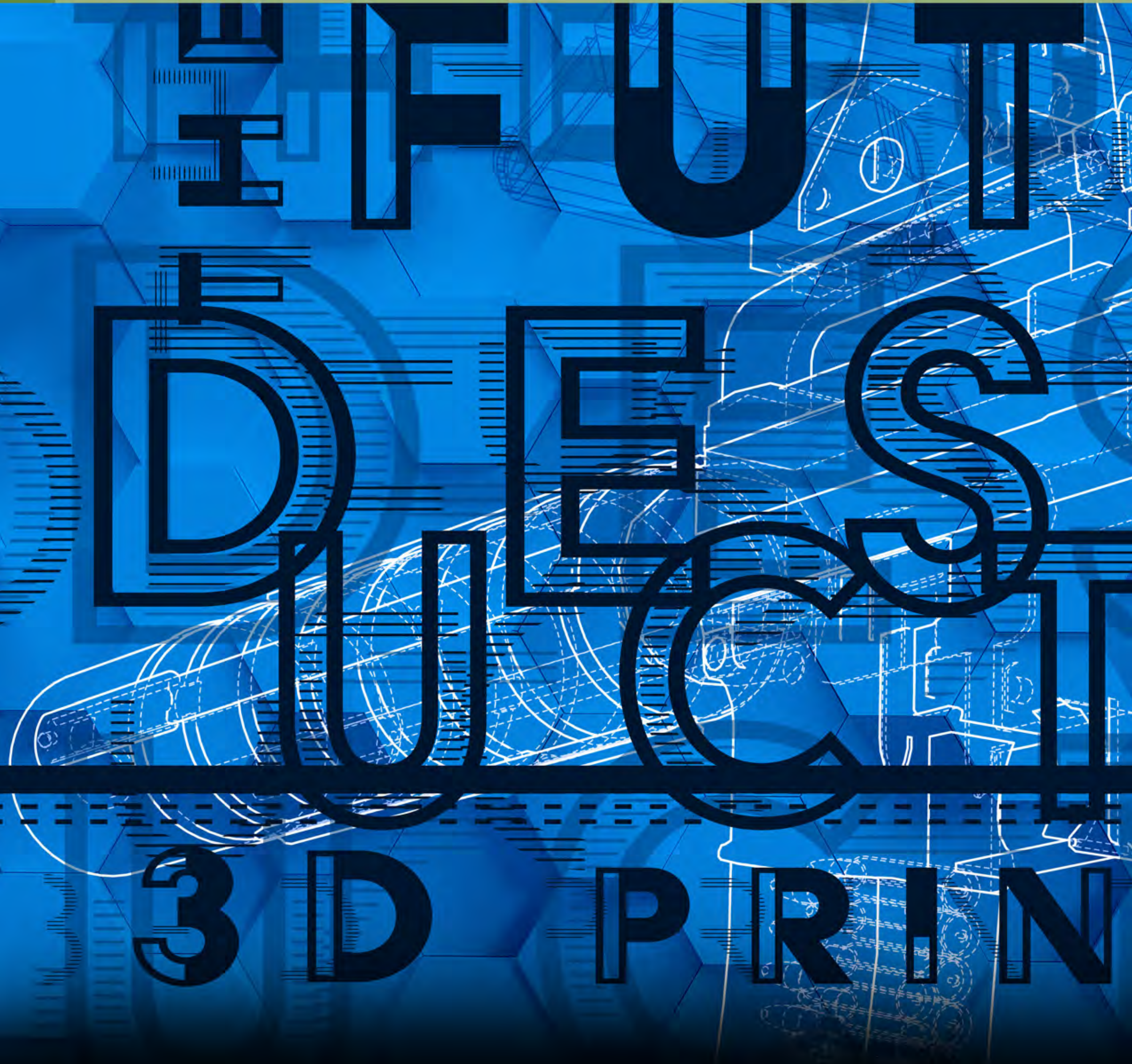
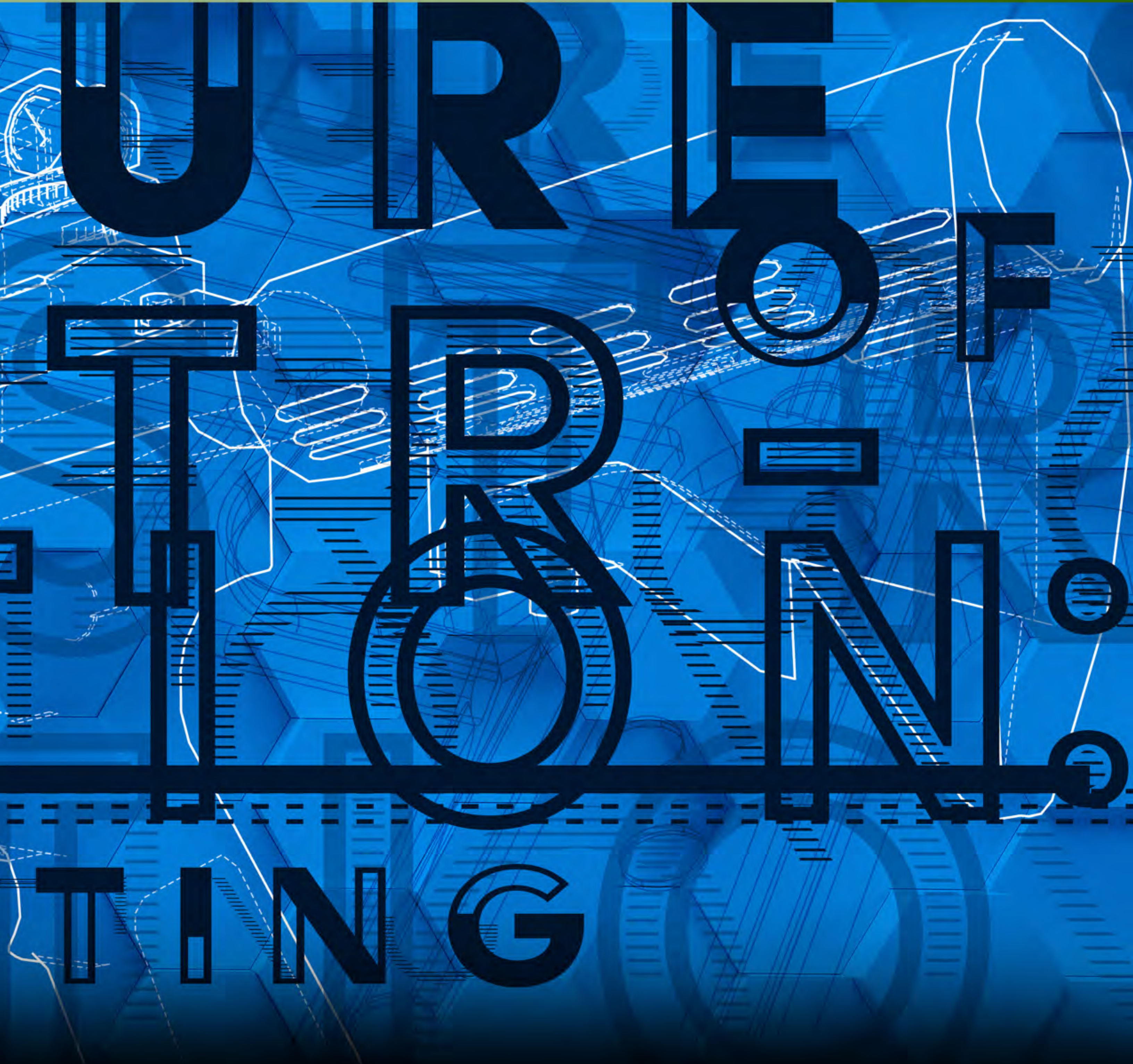


Gregory Nichols

Three-dimensional (3D) printing is rapidly being adopted by many sectors, including the U.S. Department of Defense (DoD), given its ability to reduce waste, cost, and time related to traditional subtractive manufacturing processes [1]. However, the advent of this technology, and its ability to produce objects that were previously extremely difficult to manufacture, has raised security concerns [2, 3], and many organizations have also begun to question the role that 3D printing could play in weapons development—including weapons of mass destruction (WMD).

For example, the U.K. Ministry of Defence (MoD) has acknowledged the advantages that 3D printing may present to terrorist organizations and other non-state actors in regard to weapons proliferation [4]. In 2016, DoD released its Additive Manufacturing Roadmap, which stated that, "AM [additive manufacturing] can be used to our advantage, and our adversaries can use it against us [5]." Director of National Intelligence Dan Coats echoed this sentiment in his 2018 Worldwide Threat Assessment when he remarked, "Advances in manufacturing, particularly the development of 3D printing, almost certainly will become even more accessible to a variety of state and non-state actors and be used in ways contrary to our interests [6]." During events convened by the United Nations in both 2016 and 2017, potential challenges posed by 3D printing regarding access to WMD were discussed, including an increased opportunity to "violate internation-

Image Credit Photo Illustration created by HDIAC and adapted from Adobe Stock.

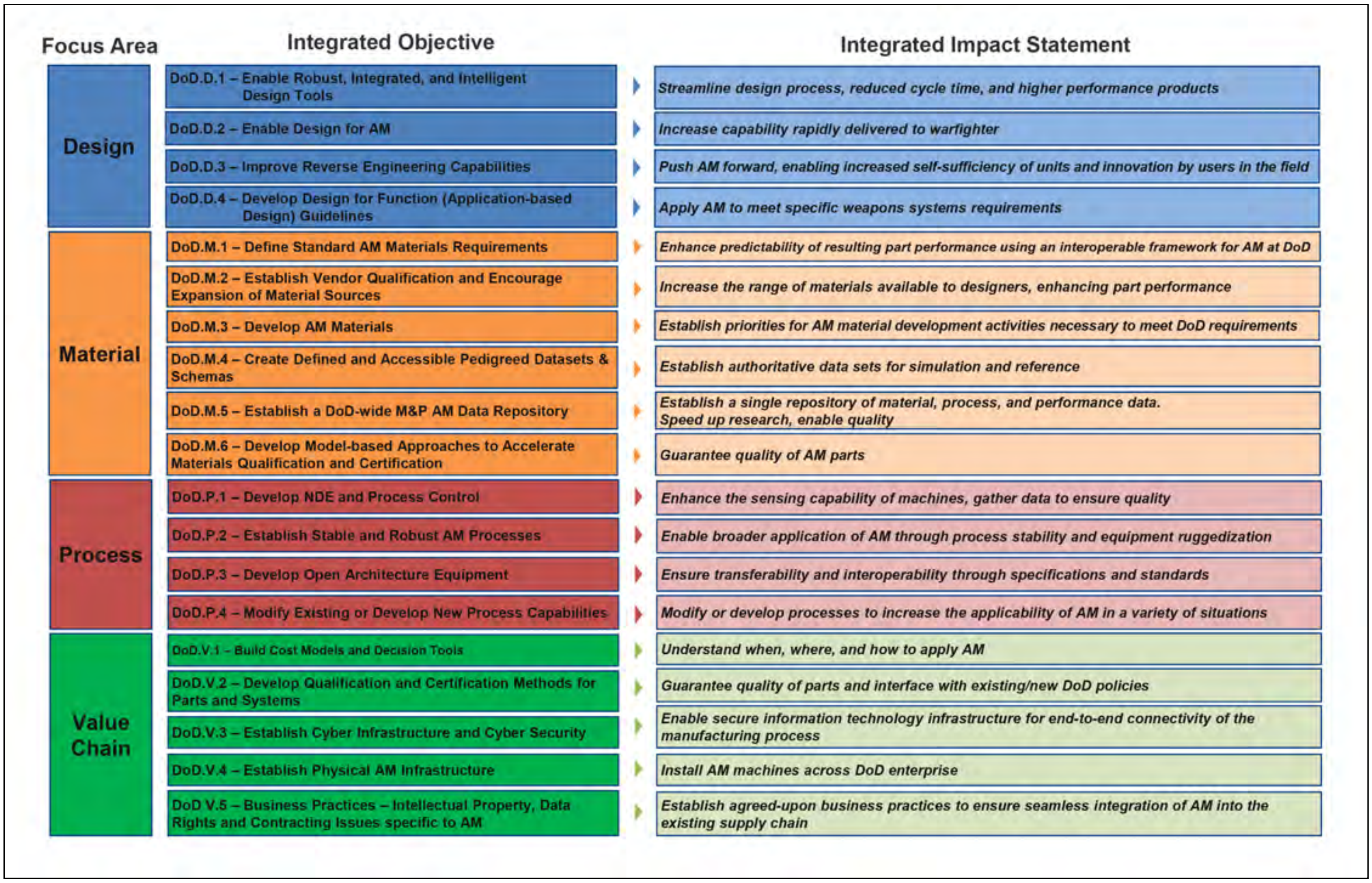


al sanctions and export controls [7],” given that it is easier to acquire such weapons by printing parts that are otherwise difficult to obtain [8]. Although 3D printing techniques continue to be refined as the technology matures, security challenges remain largely unchecked. These concerns have already been made manifest in the development of 3D printed small arms [9], consequently raising questions as to what other potentially devastating WMD or weapons of mass disruption 3D printing may harbor. Some of these concerns, including cyber vulnerabilities and counterfeit parts, have been raised by DoD and planned to be addressed as evidence by strategic objectives in DoD’s Additive Manufacturing roadmap (see Figure 1).

Overview of 3D Printing and Additive Manufacturing

3D printing “is the process of making an object by depositing materials, one tiny layer at a time [10].” The term is often used interchangeably with additive manufacturing; however, additive manufacturing can include other types of processes beyond printing [1]. Additive manufacturing techniques, including 3D printing, are in a family counterpoint to traditional manufacturing techniques, known as subtractive (e.g., forging, casting, and milling), in which material is removed from an object until the desired shape is formed [1].

The process of 3D printing is rather straightforward (see Figure 2). An object is either digitally scanned and turned into a digital file, or the design is directly created in a file. This file is imported into a machine that uses materials (e.g., metal powder or plastics) to build up a



Focus Area	Integrated Objective	Integrated Impact Statement
Design	DoD.D.1 – Enable Robust, Integrated, and Intelligent Design Tools	Streamline design process, reduced cycle time, and higher performance products
	DoD.D.2 – Enable Design for AM	Increase capability rapidly delivered to warfighter
	DoD.D.3 – Improve Reverse Engineering Capabilities	Push AM forward, enabling increased self-sufficiency of units and innovation by users in the field
	DoD.D.4 – Develop Design for Function (Application-based Design) Guidelines	Apply AM to meet specific weapons systems requirements
Material	DoD.M.1 – Define Standard AM Materials Requirements	Enhance predictability of resulting part performance using an interoperable framework for AM at DoD
	DoD.M.2 – Establish Vendor Qualification and Encourage Expansion of Material Sources	Increase the range of materials available to designers, enhancing part performance
	DoD.M.3 – Develop AM Materials	Establish priorities for AM material development activities necessary to meet DoD requirements
	DoD.M.4 – Create Defined and Accessible Pedigreed Datasets & Schemas	Establish authoritative data sets for simulation and reference
	DoD.M.5 – Establish a DoD-wide M&P AM Data Repository	Establish a single repository of material, process, and performance data. Speed up research, enable quality
	DoD.M.6 – Develop Model-based Approaches to Accelerate Materials Qualification and Certification	Guarantee quality of AM parts
Process	DoD.P.1 – Develop NDE and Process Control	Enhance the sensing capability of machines, gather data to ensure quality
	DoD.P.2 – Establish Stable and Robust AM Processes	Enable broader application of AM through process stability and equipment ruggedization
	DoD.P.3 – Develop Open Architecture Equipment	Ensure transferability and interoperability through specifications and standards
	DoD.P.4 – Modify Existing or Develop New Process Capabilities	Modify or develop processes to increase the applicability of AM in a variety of situations
Value Chain	DoD.V.1 – Build Cost Models and Decision Tools	Understand when, where, and how to apply AM
	DoD.V.2 – Develop Qualification and Certification Methods for Parts and Systems	Guarantee quality of parts and interface with existing/new DoD policies
	DoD.V.3 – Establish Cyber Infrastructure and Cyber Security	Enable secure information technology infrastructure for end-to-end connectivity of the manufacturing process
	DoD.V.4 – Establish Physical AM Infrastructure	Install AM machines across DoD enterprise
	DoD V.5 – Business Practices – Intellectual Property, Data Rights and Contracting Issues specific to AM	Establish agreed-upon business practices to ensure seamless integration of AM into the existing supply chain

Figure 1. DoD's Strategic Alignment of Objectives Regarding Development of Additive Manufacturing Capabilities [5]. (Adapted from Source: Department of Defense).

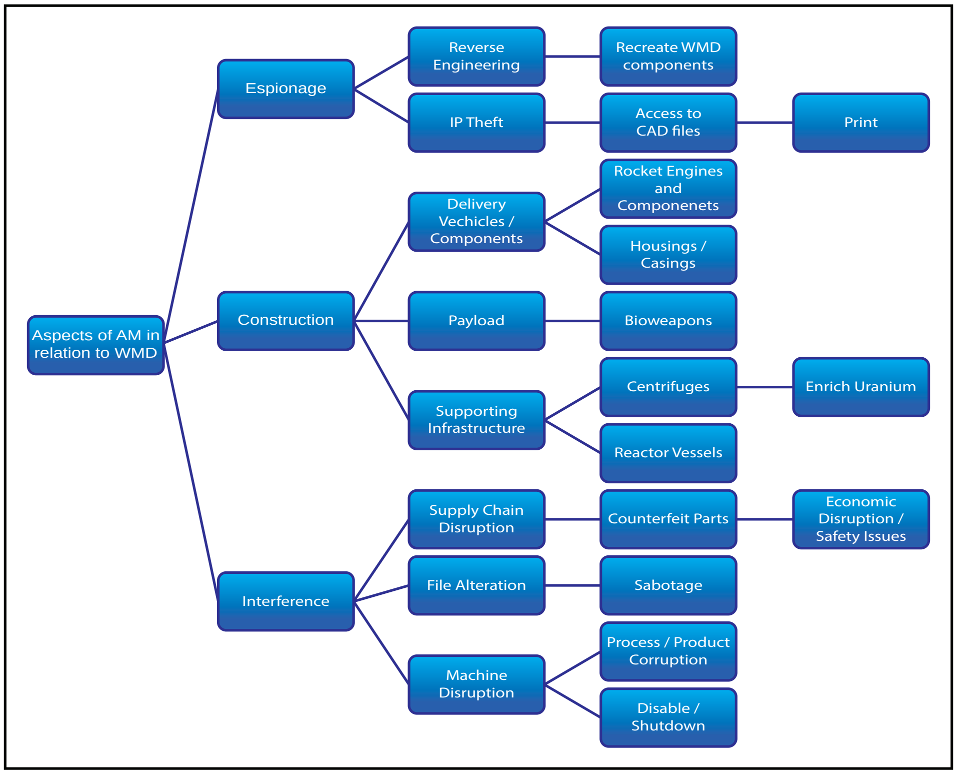


Figure 3. Classification tree demonstrating methods available to use additive manufacturing (AM) in or as a weapon of mass destruction.

3D object. Because the machine only uses the specific amount of material required to print each layer as instructed by the file, there is little to no waste.

Additional benefits afforded by this technology include a lower demand for highly skilled labor, a reduction in physical space required to house machinery compared to traditional manufacturing, and a decrease in the time required to produce objects. These benefits are also attractive to bad actors who may use 3D printing to more easily manufacture and distribute WMD—disrupting traditional barriers to WMD proliferation.

3D Printing in Relation to WMD

The potential for 3D printing to create WMD is still largely unknown, but most experts agree that it is currently unlikely that a WMD may be wholly constructed through 3D printing. However, components used to construct WMD can be 3D printed [3, 11-13]. Additionally, 3D printers and associated infrastructure (the technology itself) may be manipulated to, in effect, become weapons—more appropriately termed weapons of mass disruption [14]. This application of 3D printing for use in the development of WMD can be classified into three main categories: espionage, construction of a weapon, and interference with the 3D printing process (see Figure 3).

Espionage

According to MI5, "espionage is the process of obtaining information that is not normally publicly available ... if this information is obtained by those with no right to access it, serious damage can be caused [15]." Critical military assets manufactured by DoD laboratories and industry partners alike increasingly rely on 3D printing. Vulnerabilities in the printing process, even with restricted access, could allow this information to be gathered in one of two ways: gaining access to computer-aided design (CAD) files or conducting a side-channel attack. First, intellectual property theft is a primary concern. Since the CAD files used in 3D printing are digital, hackers could gain access to the blueprints of the item being printed, enabling the hackers to print these items or give/sell the CAD files to adversaries of the U.S. [3, 16-18]. Conversely, someone could easily scan an item and convert that image into a CAD file that could later be used in the 3D printing process [16]. The ease with which items can be copied and 3D printed replicas can be fabricated is cause for increased vigilance regarding insider threats [3, 18].

Second, based on outputs created by the 3D printing process, it is possible to reverse engineer a product—known as a side-channel attack. In 2016 and 2017, researchers at the University of California, Irvine, and Siemens Corporation published research supporting that each type of item printed on a 3D printer creates a unique pattern of "analog emissions such as vibration, acoustic, magnetic, and power [19, 20]." These emissions create a unique fingerprint for each item, and capturing these emissions makes it possible, through reverse engineering, to recreate the product being printed.

Additionally, researchers at University at Buffalo (the State University of New York) have also demonstrated that many of these emissions can easily be recorded using the sophisticated, sensitive sensors present in many smartphones [21]. Additional work by researchers at the University of California, Irvine, and Siemens Corporation was able to show that through the use of a thermal imaging camera, it is possible to trace the movement of the printer nozzle, since intense heat is used to melt the material used to form the object [22].

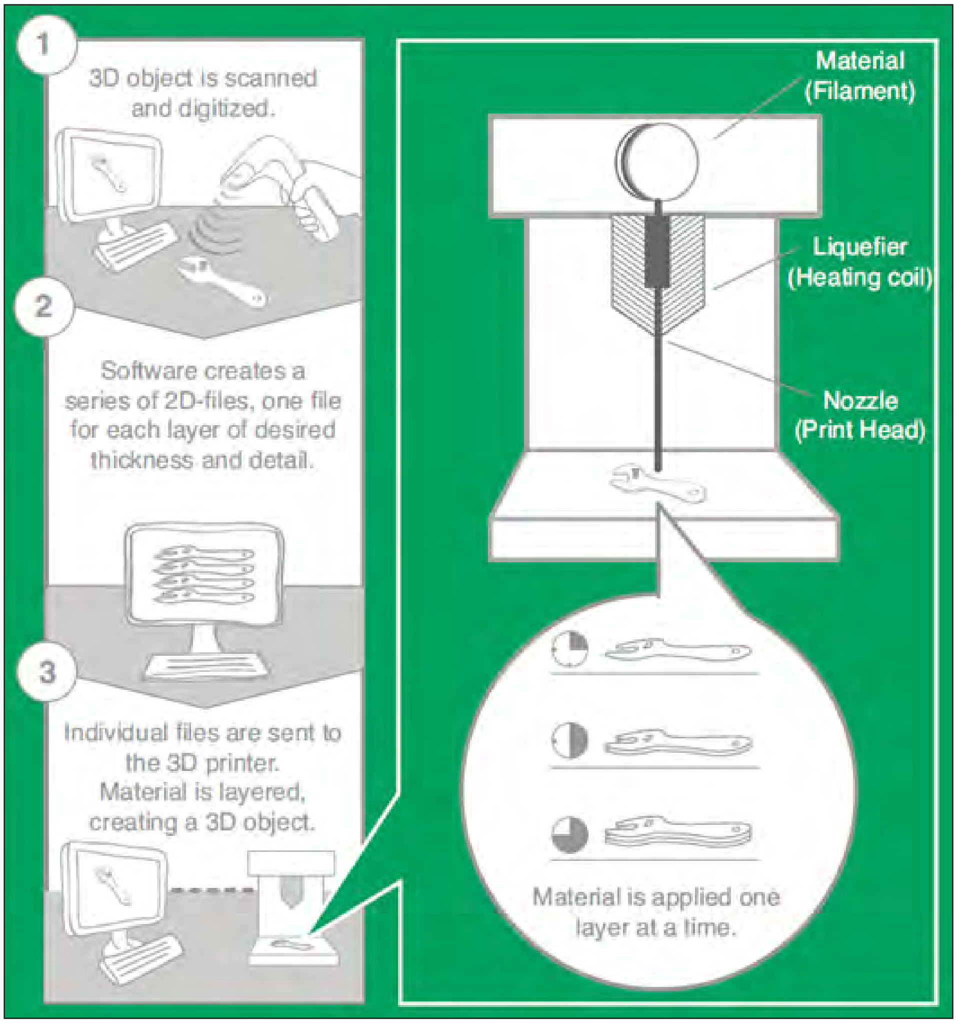

1
3D object is scanned and digitized.
2
Software creates a series of 2D-files, one file for each layer of desired thickness and detail.
3
Individual files are sent to the 3D printer. Material is layered, creating a 3D object.
Material (Filament)
Liquefier (Heating coil)
Nozzle (Print Head)
Material is applied one layer at a time.

Figure 2. Overview of the additive manufacturing process [2] (Released).

Construction

Traditional barriers to creating WMD include export controls, limited access to specialized resources, time, scale of facilities needed, and volume of waste produced [23]. One of the key advantages, and also concerns, of 3D printing is that it removes some of these barriers. Several key components of a WMD could be printed [11, 13], including delivery vehicles/components (e.g., missiles and engine components), some payloads (i.e., chemical and limited biological), and supporting infrastructure to make the payloads or WMD (e.g., centrifuges for uranium enrichment). However, at this time, 3D printing could not be used to print an entire WMD or even all components (i.e., nuclear payloads) [11-13].

Many governmental, academic, and industrial organizations have conducted research regarding the 3D printing of rocket and missile components. Organizations, including NASA, Aerojet Rocketdyne, and SpaceX have all successfully launched rockets comprised of smaller 3D printed components, such as valves [24, 25]. Furthermore, in 2016, students at the University of California, San Diego, launched a rocket, the Vulcan-1, which featured a completely 3D printed engine [25].

Raytheon Missile Systems has already demonstrated it is possible to 3D print almost every component of a missile, including rocket engines, fins, and parts for guidance and control systems [26]. The technology continues to develop, which may allow soldiers to print and assemble missiles in the field. In terms of traditional concepts of WMD delivery systems, Lockheed Martin is exploring potential uses of 3D printing for next generation intercontinental ballistic missiles [27].

The printing of payloads and support infrastructure is currently more complicated than the 3D printing of launch vehicles—thereby making it less likely to occur. One of the biggest debates over the past few years has been whether it is possible to 3D print an entire nuclear weapon. Researchers from academia and the non-gov-

Challenges	Solution	Performing Organization(s)
Counterfeiting	Embed quantum dots in object	Quantum Materials Corp [48]
File tampering	Hashing/blockchain	Virginia Polytechnic Institute and State University [37]
Counterfeiting	Add taggant to source material	Electric Power Research Institute [44]
Counterfeiting	Micro/nano-strctured fingerprints/watermarks	U.S. Department of Defense [5]
Sabotage/Counterfeiting/Quality Control	Mechanical and physical testing	New York University and University of Texas[38]
Illegal access to materials	Monitor online retailers	Wisconsin Project on Nuclear Arms Control [43]
Sabotage/Counterfeiting/Quality Control	Three-layer verification	Georgia Institute of Technology and Rutgers University [49]
Sabotage/Counterfeiting/Quality Control	Piezoelectric transducer augment impendence-based structural health monitoring	Virginia Polytechnic Institute and State University [50]
Sabotage	Continuous monitoring of current delivered to actuators	University of South Alabama, Ben-Gurion University, Lawrence Livermore National Laboratory, and Singapore University of Technology and Design [51]
Sabotage	Digital audio signing	Ben-Gurion University, University of South Alabama, and Singapore University of Technology and Design [42]
Weapons proliferation	Explore possibilities for 3D printing weapons	Terrorist Explosive Device Analytical Center [47]
Intellectual property protection/Counterfeiting	Spectral signatures	InfraTrac, The Pennsylvania State University and the University of Maryland [52]

Table 1: Proposed methods for mitigating challenges of 3D printing in the development of WMD.

ernmental organization sector with previous government and policy experience agree the technology does not fully support the ability to print an entire nuclear weapon [11-13]. One of the key challenges is printing the core due to the complicated chemistries of uranium, plutonium, and beryllium [11].

However, one crucial component, high-yield explosives, has been printed on at least two occasions at Department of Energy (DOE) laboratories —Los Alamos National Laboratory and Lawrence Livermore National Laboratory [28, 29]. To some degree, it is possible to print smaller components of nuclear weapons. It may also be possible to print parts of reactors [11] and centrifuges since additive manufacturing technology improves every day. For example, it is becoming possible to print with critical materials, such as carbon fiber and maraging steel, which are required in the construction of centrifuges [13].

A partnership between Lawrence Livermore National Laboratory and Y-12 National Security Complex supports the National Nuclear Security Administration in finding new methods to update the nuclear weapons enterprise using additive manufacturing [30]. In addition, DOE, the Electric Power Research Institute, and various industry partners are exploring additive manufacturing methods to create nuclear reactor components [31].

Chemical and biological agents are more difficult to 3D print, but the technology is rapidly developing to accommodate these capabilities. For example, researchers at the Middlebury Institute of International Studies in Monterey, California, explain that 3D printing may allow for the construction of tissues needed to perform toxicity testing for biological agents [32], and researchers from Louisiana State University estimate that it could be possible to print simple chemical weapons in 10 years [33].

Interference

Interference can be more accurately defined as disruption, rather than the conventional view of destruction. The interface of cyber-based and online controls with physical objects, known as cyber-physical systems, is becoming more commonplace, particularly among critical infrastructure sectors. Concerns regarding the effects of interrupting cyber-physical systems used in critical infrastructure can be traced to at least 1997, when the President's Commission on Critical Infrastructure Protection reported that "disruption of any infrastructure is always inconvenient and can be costly and even life threatening [34]."

3D printers are sometimes directly connected to the internet, are used in large-scale production facilities that are connected to extensive computer-based control systems, and rely on digital files—making them vulnerable to attack [35]. Apart from security concerns related to cyberattacks that could shut down 3D printers used in the Defense Industrial Base and Critical Manufacturing Sectors [36], disruption of cyber-physical systems in manufacturing could lead to major disruption among other sectors, including the Nuclear Reactors, Materials, and Waste Sector; the Chemical Sector; and the Transportation Sector.

Concerns related to the manipulation of 3D printed parts in these critical sectors can come in three forms. First, bad actors could deliberately manipulate CAD files so that crucial components would fail during operation, leading to catastrophic error in a system [37]. Sabotage could occur by altering the printing orientation of the object or embedding defects into the object [38]. This is a key concern within the aviation industry as an influx of companies, such as Boeing, Airbus, and GE Aviation, are utilizing 3D printed components [39]. In fact, this could also be a concern for military aircraft security as earlier this year, Marines aboard the USS Wasp successfully 3D printed a replacement part for an F-35B Lightning II [40]. Moreover, academic researchers demonstrated the ease of sabotage in 2016 when they altered the file for one of the propellers on a quadrotor drone, causing the propeller to fail during the test flight, crashing the drone [41].

Second, since many 3D printers are connected to the internet, or to a networked computer system, several researchers have also theorized it is possible to hack directly into the printer, causing it to malfunction [37, 42]. This threat has been acknowledge by DoD, and developing safeguards to prevent cyberattacks on 3D printers is identified as an objective in the DoD Additive Manufacturing Roadmap [5]. Finally, the ease of access to 3D printers and the materials they need to fabricate items makes it much easier for both legitimate users and underground operators to produce parts intended for critical sectors [43]. Counterfeit parts, particularly in the nuclear industry, have been tracked for many years [44]. However, the advent of 3D printing will most likely improve the ease with which counterfeit parts can be produced, yielding parts whose flaws remain nearly undetectable. These counterfeit parts pose safety and security concerns as they may more readily enter legitimate supply chains [2, 23, 45].

Research Gaps, Challenges, and Mitigation

A 2018 National Defense University study found that additive manufacturing will have a much greater impact than other emerging technologies on acquisition, production, weaponization, and delivery of WMD [46]. Because of this, many researchers and agencies are developing strategies to address critical safety and security gaps. These efforts have been placed into five categories by Fey [3]:

- Strengthening cybersecurity related to 3D printers and supporting infrastructure

- Incorporating protective measures directly within software, hardware, and materials

- Adapting export controls to minimize the purchase and use of new 3D printing technology and base materials that could be used to create WMD

- Raising awareness of the new challenges 3D printing brings to WMD proliferation

- Encouraging industry to impose self-regulation/best-practices regarding the responsible use of 3D printing technologies

The DoD acknowledges the cyber risks posed by 3D printers and has included objectives to strengthen this area in its Additive Manufacturing Roadmap [5]. Other areas of risk, such as sabotage and counterfeiting, are being addressed by researchers across academia, industry, and government, who are primarily investigating methods to embed identifying materials in 3D printed objects for easy detection of tampering (see Table 1).

However, the use of 3D printing to circumvent export controls remains one of the most difficult challenges to address. Critical materials (e.g., maraging steel, titanium, and carbon fiber) are widely available for purchase online [43], and while the high-precision CNC machines needed to create components of nuclear weapons are export-controlled, 3D printers are not. The technological ability of many 3D printers that use metal powders could be precise enough to print several components needed for nuclear weapons production [13].

Closing export control gaps is crucial to national security. In 2014, the FBI's Terrorist Explosive Device Analytical Center (TEDAC) purchased a 3D printer to investigate the types of explosive devices that can be made with printers and printing materials easily purchased online. This effort allows the agency to better understand the capabilities that 3D printing may provide to terrorists and insurgents [47]. Actions such as TEDAC's may support other agencies, including DoD, in understanding the emerging capabilities 3D printing brings to WMD proliferation. It can also aid in the development of 3D printing-specific counterproliferation techniques.

Conclusion

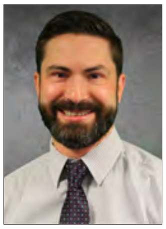
3D printing has already been used to create small arms that can fire bullets with relative precision [9], and additional uses in weapons development will continue to take shape as the technology advances. As the level of sophistication regarding 3D printing grows, so will the risk attributed to non-state actors in weapons proliferation and WMD creation. The DoD and Department of Homeland Security have both acknowledged these risks, but the rapid pace of technology development and existing policies that were created to address traditional WMD threats (i.e., nuclear weapons made with conventional means) do not necessarily provide all the resources needed to mitigate new threats. However, DoD has acknowledged some of these challenges and is working toward solutions, primarily securing cyber-physical infrastructure and reducing the risk of sabotage.

References

1. U.S. Government Accountability Office. (2015, October). Defense additive manufacturing: DoD needs to systematically track department-wide 3D printing efforts (GAO-16-56). Washington, DC. Retrieved from https://www.gao.gov/assets/680/673099.pdf
2. McNulty, C. M., Arnas, N., & Campbell, T. A. (2012). Toward the printed world: Additive manufacturing and implications for national security (Defense Horizons Policy Brief No. 73). Washington, DC: National Defense University, Institute for National Strategic Studies. doi:10.21236/ada577162
3. Fey, M. (2017). 3D printing and international security: Risks and challenges of an emerging technology (PRIF Rep. No. 144). Frankfurt am Main, Germany: Peace Research Institute. Retrieved from https://www.hsfk.de/fileadmin/HSFK/hsfk_publikationen/prif144.pdf
4. Ministry of Defence U.K. (2015). Strategic Trends Programme: Future operating environment 2035 (1st ed., Development, Concepts and Doctrine Centre Strategic Trends Programme, MOD Guidance). Ministry of Defence U.K. Retrieved from https://www.gov.uk/government/publications/future-operating-environment-2035
5. U.S. Department of Defense. (2016, November 30). Department of Defense Additive Manufacturing Roadmap (Final Rep.). Retrieved from https://myclass.dau.mil/bbcswebdav/institution/Courses/Deployed/ACQ/ACQ404/Archives/Student%20Materials/Student_Materials/6%20SAMC%20Class%20Prep%20Readings%20-%20FY17-2%20June%205-9/Additional%20References/DoD%20Nov%2016%20Rpt%20Re%20Additive%20Manufacturing%20Roadmap.pdf?uniq=d3jpcp&version=1
6. Statement for the record: Worldwide threat assessment of the U.S. Intelligence Community (2018) (testimony of Daniel R. Coats, Director of National Security). Retrieved from https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community
7. United Nations Office for Disarmament Affairs. (2016, October 14). Emerging technology, international security, and international law. Retrieved from https://www.un.org/disarmament/update/emerging-technology-international-security-and-international-law/
8. United Nations. (2017, June 28). International cooperation key to keeping WMDs away from terrorists, Security Council told. Retrieved from https://news.un.org/en/story/2017/06/560512-international-cooperation-key-keeping-wmds-away-terrorists-security-council
9. Walther, G. (2015). Printing insecurity? The security implications of 3D-printing of weapons. Science and Engineering Ethics, 21(6), 1435-1445. doi:10.1007/s11948-014-9617-x
10. U.S. Department of Energy. (2014, June 19). How 3D printers work. Retrieved from https://www.energy.gov/articles/how-3d-printers-work
11. Kelley, R. (2017). Is three-dimensional (3D) printing a nuclear proliferation tool? (Non-Proliferation Papers No. 54). EU Non-Proliferation Consortium. Retrieved from https://www.sipri.org/publi-

cations/2017/eu-non-proliferation-papers/three-dimensional-3d-printing-nuclear-proliferation-tool

12. Kroenig, M., & Volpe, T. (2015). 3D printing the bomb? The nuclear nonproliferation challenge. The Washington Quarterly, 38(3), 7-19. doi:10.1080/0163660x.2015.1099022
13. Christopher, G. (2015). 3D printing: A challenge to nuclear export controls. Strategic Trade Review, 1(1), 18-25. Retrieved from http://www.str.ulg.ac.be/wp-content/uploads/2016/01/2_3D_Printing_A_Challenge_to_Nuclear_Export_Controls.pdf
14. Bunker, R. J. (2000). Weapons of mass disruption and terrorism. Terrorism and Political Violence, 12(1), 37-46. doi:10.1080/09546550008427548
15. MI5 - The Security Service. (n.d.). Espionage. Retrieved from https://www.mi5.gov.uk/espionage
16. Dijkstra, M., Krause, A., Masri, L., McCambridge, G., Ng, J., Pek, S.B., Yang, E.S., & Zheng, Y. (2014). U.S. National Strategy for Additive Manufacturing. 2014 Capstone Project. Yale Jackson Institute for Global Affairs. Retrieved from https://cgsr.llnl.gov/content/assets/docs/AMCapstone_Final.pdf
17. Holbrook, T. R., & Osborn, L. (2014). Digital patent infringement in an era of 3D printing. SSRN Electronic Journal. doi:10.2139/ssrn.2483550
18. Andrews, J. W. (2017). Additive manufacturing: Implications for the interagency's nuclear counterproliferation task. InterAgency Journal, 8(2), 7-16. Retrieved from http://thesimonscenter.org/iaj-8-2-2017/
19. Chhetri, S. R., & Faruque, M. A. (2017). Side channels of cyber-physical systems: Case study in additive manufacturing. IEEE Design & Test, 34(4), 18-25. doi:10.1109/mdat.2017.2682225
20. Faruque, M. A., Chhetri, S. R., Canedo, A., & Wan, J. (2016). Acoustic side-channel attacks on additive manufacturing systems. 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS). doi:10.1109/iccps.2016.7479068
21. Song, C., Lin, F., Ba, Z., Ren, K., Zhou, C., & Xu, W. (2016). My smartphone knows what you print. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS16. doi:10.1145/2976749.2978300
22. Al Faruque M. A., Chhetri, S. R., Faezi, S., & Candeo, A. (2016). Forensics of thermal side-channel in additive manufacturing systems (CECS Technical Report #16-01). Retrieved from https://pdfs.semanticscholar.org/c8ca/d6066871137ecca3003d35b6111ea4107ba2.pdf
23. Bajema, N.E. & DiEuliss, D. (2016). Peril and promise: Emerging technologies and WMD (Emergence and Convergence Workshop Report). National Defense University. Retrieved from http://wmdcenter.ndu.edu/Publications/Publication-View/Article/1181150/peril-and-promise-emerging-technologies-and-wmd/
24. Brockmann, K., & Bauer, S. (2017, November). 3D printing and missile technology controls (Stockholm International Peace Research Institute Background Paper). Retrieved from https://www.sipri.org/publications/2017/sipri-background-papers/3d-printing-and-missile-technology-controls
25. Atherton, K. D. (2016, May 25). University students launched a rocket with completely 3D-printed engine. Popular Science. Retrieved from https://www.popsci.com/university-students-launch-rocket-with-3d-printed-engine
26. Raytheon. (2017, December 11). To print a missile - Raytheon research points to 3D printing for tomorrow's technology. Retrieved from https://www.raytheon.com/news/feature/print-missile
27. Insinna, V. (2017, April 3). Lockheed pitches 3D printed parts for next-generation ICBM program. Retrieved from https://www.defensenews.com/digital-show-dailies/space-symposium/2017/04/03/lockheed-pitches-3D-printed-parts-for-next-generation-icbm-program/
28. Hutterer, E. (2016, March). Explosive 3D design: 3D printing could revolutionize the high-explosives industry. 1663, 2-5. Retrieved from https://www.lanl.gov/discover/publications/1663/2016-march/_assets/docs/1663_26.pdf
29. Gash, A. (2015). High-explosive components using advanced manufacturing methods. FY2015 LDRD Annual Report. Retrieved from https://ldrd-annual.llnl.gov/ldrd-annual-2015/materials/components
30. 30. Hansen, R. (2015, January/February). Next-generation manufacturing for the stockpile. Science & Technology Review, 4-11. Retrieved from https://str.llnl.gov/january-2015/marrgraff
31. 31. Barker, B. (2017, May/June). A "moonshot" for reactor vessel production. EPRI Journal, 2, 5-8. Retrieved from http://eprijournal.com/a-moonshot-for-reactor-vessel-production/
32. 32. Zilinskas, R.A. & Mauger, P. (2015). Biotechnology e-commerce: A disruptive challenge to biological arms control (CNS Occasional Paper No. 21). Middlebury Institute of International Studies at Monterey. Monterey, CA. Retrieved from http://www.nonproliferation.org/wp-content/uploads/2015/06/biotech_ecommerce.pdf
33. 33. Tirone, D. C., & Gilley, J. (2015). Printing power: 3D printing and threats to state security. Journal of Policing, Intelligence and Counter Terrorism, 10(2), 102-119. doi:10.1080/18335330.2015.1089636
34. President's Commission on Critical Infrastructure Protection. (1997). Critical foundations: Protecting America's infrastructures (Rep.). Retrieved from https://www.hsdl.org/?abstract&did=986
35. Desmit, Z., Elhabashy, A. E., Wells, L. J., & Camelio, J. A. (2017). An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. Journal of Manufacturing Systems, 43, 339-351. doi:10.1016/j.jmsy.2017.03.004
36. U.S. Department of Homeland Security. (2017, July 11). Critical Infrastructure Sectors. Retrieved from https://www.dhs.gov/critical-infrastructure-sectors
37. Sturm, L. D., Williams, C. B., Camelio, J. A., White, J., & Parker, R. (2017). Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects. Journal of Manufacturing Systems, 44, 154-164. doi:10.1016/j.jmsy.2017.05.007
38. Zeltmann, S. E., Gupta, N., Tsoutsos, N., G., Maniatakos, M., Rajendran, J., & Karri, R. (2016). Manufacturing and security challenges in 3D printing. JOM, 68(7), 1872-1881. doi:10.1007/s11837-016-1937-7
39. Cooper, P. (2017). Aviation cybersecurity: Finding lift, minimizing drag (Rep.). Atlantic Council. Retrieved from http://www.atlanticcouncil.org/publications/reports/aviation-cybersecurity-finding-lift-minimizing-drag
40. Mendez, S. (2018, April 19). Marines Use 3D Printer to Make Replacment Part for F-35 Fighter. Retreived from https://www.defense.gov/News/Article/Article/1498121/.
41. Belikovetsky, S., Yampolskiy, M., Toh, J., & Elovici, Y. (2016). dr0wned – Cyber-physical attack with additive manufacturing. Retrieved from https://arxiv.org/abs/1609.00133
42. Belikovetsky, S., Solewicz, Y., Yampolskiy, M., Toh, J., & Elovici, Y. (2017). Detecting cyber-physical attacks in additive manufacturing using digital audio signing. Retrieved from https://arxiv.org/abs/1705.06454
43. Clover, C. (2014, September 26). Alibaba: Weapons of mass ecommerce. The Financial Times. Retrieved from https://www.ft.com/content/2a19e07c-43ef-11e4-8abd-00144feabdc0
44. Tannenbaum, M. (2015, June). Counterfeit and fraudulent parts: Improving prevention and detection. Nuclear News, 58(13), 46-49. Retrieved from www.ans.org/pubs/magazines/download/a_981
45. Deloitte. (2017). 3D opportunity for adversaries: Additive manufacturing considerations for national security (Rep.). Deloitte University Press. Retrieved from https://www2.deloitte.com/content/dam/insights/us/articles/3847_3D-opportunity-for-adversaries/DUP_3D-opportunity-for-adversaries.pdf
46. Bajema, N. E. (2018). Emergence & convergence: Risk assessment survey (Rep.). National Defense University. Retrieved from http://wmdcenter.ndu.edu/Media/News/Article/1484495/emergence-and-convergence/
47. Halterman, T. (2014, June 24). FBI to use 3D printing for bomb research. Retrieved from http://www.3dprinterworld.com/article/fbi-use-3d-printing-for-bomb-research
48. Taylor, P. (2014, July 1). Anti-counterfeit tech developed for 3D-printed objects. Retrieved from https://www.securingindustry.com/electronics-and-industrial/anti-counterfeit-tech-developed-for-3d-printed-objects/s105/a2075/#.WtdLQS7wZEY
49. Bayens, C., Le, T., Garcia, L., Beyah, R., Javanmard, M., & Zonouz, S. (2017). See no evil, hear no evil, feel no evil, print no evil? Malicious fill pattern detection in additive manufacturing. In Proceedings of the 26th USENIX Security Symposium (pp. 1181-1198). Retrieved from https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-bayens.pdf
50. Vincent, H., Wells, L., Tarazaga, P., & Camelio, J. (2015). Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems. Procedia Manufacturing, 1, 77-85. doi:10.1016/j.promfg.2015.09.065
51. Moore, S. B., Gatlin, J., Belikovetsky, S., Yampolskiy, M., King W. E., & Elovici, Y. (2017). Power consumption-based detection of sabotage attacks in additive manufacturing. Retrieved from https://arxiv.org/abs/1709.01822.
52. Flank, S., Nassar, A. R., Simpson, T. W., Valentine, N., & Elburn, E. (2017). Fast Authentication of Metal Additive Manufacturing. 3D Printing and Additive Manufacturing, 4(3), 143-148. doi:10.1089/3dp.2017.0018.



Gregory Nichols, MPH, CPH
Subject Matter Expert, HDIAC

Gregory Nichols is an HDIAC Subject Matter Expert. Previously, he managed the Nanotechnology Studies Program at ORAU in Oak Ridge, Tennessee, where he provided expertise on nanotechnology-related topics and conducted research. Prior to ORAU, Nichols spent 10 years in various healthcare roles including five years as a hospital corpsman in the U.S. Navy. He has published and presented on a variety of topics including nanotechnology, public health, and risk assessment. He has a bachelor's degree in philosophy and a Master of Public Health degree, both from the University of Tennessee, and holds the Certified in Public Health credential.