HOMELAND SECURITY ADVISORY COUNCIL

FINAL REPORT OF THE EMERGING TECHNOLOGIES SUBCOMMITTEE

3D-PRINTING

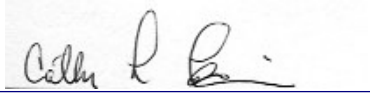
February 24, 2020

This page is intentionally left blank

This publication is presented on behalf of the Homeland Security Advisory Council, Emerging Technologies Subcommittee, under Co-Chair Thad Allen, and Co-Chair Cathy Lanier and Vice Chair Robert Rose as the ***final report*** and recommendations to the Acting Secretary of the Department of Homeland Security, Chad F. Wolf, regarding 3D Printing.

<SIGNATURE OBTAINED FOR PDF COPY>

Thad Allen (Co-Chair)



Cathy Lanier (Co-Chair)

Robert Rose (Vice-Chair)

This page is intentionally left blank.

EMERGING TECHNOLOGIES SUBCOMMITTEE

Thad Allen (Co-Chair) – Executive Vice President, Booz Allen Hamilton
Cathy Lanier (Co-Chair) – Senior Vice President and Chief Security Officer, National Football League
Robert Rose (Vice-Chair) – Founder and President, Robert N. Rose Consulting LLC
Frank Cilluffo – Director, McCrary institute for Cybersecurity and Critical Infrastructure Protection, Auburn University
Mark Dannels – Sheriff, Cochise County Arizona
Carie Lemack – Co-Founder and CEO, DreamUp
Jeffrey Miller – Vice President of Security, Kansas City Chiefs

HOMELAND SECURITY ADVISORY COUNCIL STAFF

Mike Miron, Acting Executive Director, Homeland Security Advisory Council
Evan Hughes, Associate Director, Homeland Security Advisory Council

This page is intentionally left blank.

TABLE OF CONTENTS

This page is intentionally left blank.

EXECUTIVE SUMMARY

The accelerated pace of technological change in today's global research and development ecosystem creates both risk and opportunity within the Department of Homeland Security's (DHS) mission domain. While emerging technologies may comprise powerful capabilities that can be used by operational end users, they may also pose threats for which no effective countermeasures readily exist. The challenge of addressing emerging technological threats to the Homeland while simultaneously acquiring and deploying capabilities to meet new threats is of paramount importance now and in the foreseeable future. This report provides an assessment of the current state and perceived future advancements over the next 3-10 years that could pose a threat to the homeland security of the United States, as well as recommendations for mitigation.

Evolving legal frameworks, such as the recently-passed FAA Reauthorization, provide new authorities; however, they also increase the complexity of implementing policy and deployment capabilities across the federal government and within DHS. Additional difficulties arise when implementation must be coordinated with state, local, tribal, and territorial (SLTT) authorities.

The global research and development ecosystem that exists today continues to accelerate the pace of technology introduction and maturation. While the results currently appear to be holistically positive for mankind, rapid technological advancement poses both a threat and an opportunity to U.S. national security for which the U.S. Department of Homeland Security (DHS) is charged to protect. Emerging technologies could pose threats for which no effective countermeasure readily exists, or they may comprise a powerful new enabling technology that can be used by operational end-users. In today's fast-changing and complex threat environment, the ability to both avoid and harness technology is of prime importance to the mission of homeland security.

The landscape of emerging technologies is immense, yet DHS Science &Technology's (S&T's) technology monitoring keeps tabs on many of the most promising and impactful technologies. The House Security Advisory Council (HSAC) is charged with exploring six emerging technologies and developing recommendations to take advantage of them and to minimize how U.S. adversaries can and might use these technologies against the United States. The six emerging technologies include:

- unmanned aerial and ground-based systems (UAS),
- artificial intelligence and machine learning,
- 3D printing
- synthetic biology and gene editing, and
- quantum information science and quantum computing.

The following sections define each technology, discuss the emerging features and functionality that will arise, propose some candidate use cases for the technology in the homeland security domain, and describe some of the impediments to the deployment of the technology.

This page is intentionally left blank.

1. Assessment of the current state and perceived future advancements over the next 3-10 years that could pose a threat to the homeland security of the United States.

1.1 Current State of 3D Printing Technology

3D printing and additive manufacturing (AM) are defined in ISO/ASTM 52900.[1] AM is defined as a process that builds parts from a 3D digital model layer-by-layer rather than cutting unwanted material away (termed "subtractive manufacturing"). 3D printing is defined as "fabrication of objects through the deposition of a material using a print head, nozzle, or another printer technology." Historically, the term 3D printing (as opposed to AM) was associated with machines that were lower in price and/or overall capability. Today, the term is commonly used interchangeably with AM.

The 3D printing industry has grown rapidly over the course of the past ten years, spurred by the expiration of key patents allowing new companies to enter the industry. At present, the revenue associated with 3D printing products and services totals more than $6 billion annually. The history and rapid growth of the industry over recent years is captured in Figure 3.

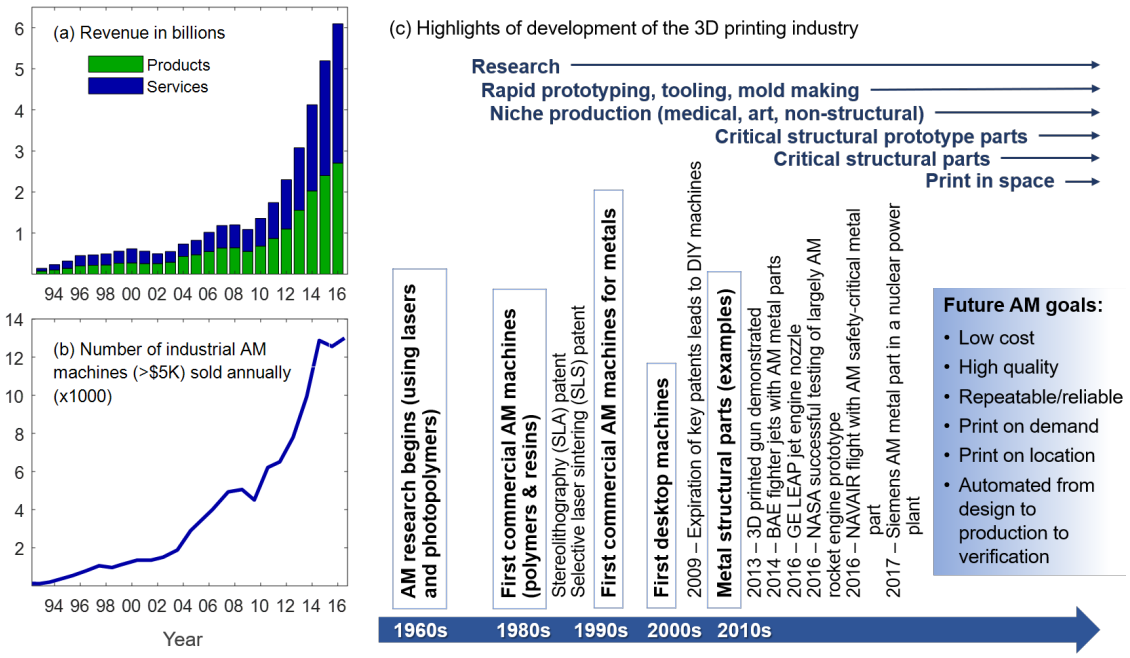


Figure 3: Development of the 3D Printing Industry

Current methods for 3D printing fall under seven process categories defined by ISO/ASTM

[1] ISO/ASTM 52900, "Standard Terminology for Additive Manufacturing - General Principles - Terminology," ISO/ASTM, 2015.

52900. These processes are detailed in Figure 4.

Process	Synonyms	Description	Applicable Materials
Material Extrusion	• Fused Deposition Modeling (FDM) • Fused Filament Fabrication (FFF) • Plastic Jet Printing (PJP)	Polymer is extruded through a heated nozzle onto a support structure or the workpiece	Thermoplastics, e.g. • ABS • PLA • Nylon • Ultem
Material Jetting	• Multijet Modeling (MJM) • Droplet-on-Demand	Droplets of build material are selectively deposited onto a build bed to produce a 3-dimensional object	Polymers and waxes, e.g. • Polypropylene • HDPE • PS • PMMA • PC • ABS
Vat photo-polymerization	• Stereolithography (SLA) • Resin Printing • Optical Fabrication	Liquid photopolymer in a vat is selectively cured by light-activated polymerization	Photosensitive polymers
Powder Bed Fusion (PBF)	• Selective Laser Sintering or Melting (SLS or SLM) • Direct Metal Laser Sintering (DMLS)	Thermal energy selectively fuses regions of a powder bed to build up parts	Uniform powders • Metal • Polymer
Directed Energy Deposition (DED)	• Laser Engineered Net Shaping (LENS) • Direct Metal Deposition (DMD) • Laser Consolidation (LC)	Focused thermal energy fuses materials by melting them as they are deposited	Metal powders • Uniform • Varying composition (gradient materials)
Binder Jetting	• Inkjet Powder Printing	Powder material is bonded selectively using a liquid bonding agent	• Metal powders • Plastic powders • Sand
Sheet Lamination	• Laminated Object Manufacturing (LOM)	Sheets of material are bonded together to form a 3-dimensional object	• Paper • Metal foils • Plastic

	• Ultrasonic Consolidation		

Figure 4: 3D Printing Process Categories as Defined by ASTM/ISO 52900

Machine price points span the range of a few hundred dollars for low-end hobbyist systems to over $500,000 for high-end industrial systems. Figure 5 illustrates the range of 3D printing systems costs and typical applications at various price points.

Figure 5: Range of 3D Printing System Costs and Use Cases

1.2 Expected Advancements of 3D Printing Technology

As the rapid growth of the 3D printing industry continues, the technology is reaching more users and application spaces. When considering the future of the industry from the perspective of homeland security, a number of relevant expected advancements arise, which are detailed below.

Decreasing Cost of Metal Printing

Timeframe: 0-5 years

The cost of metal printing technologies has recently seen some decreases, and it is expected that with these decreases such processes will gradually become broadly available. Companies, including Markforged and Desktop Metal, have developed and brought to market systems at a significantly lower price point than that of laser- or electron beam-based sintering/melting systems. These newer, lower cost systems bind metal powder in a polymer matrix to form a part, which is subsequently sintered in a furnace. In addition to the lower cost of the system itself, the metal powders used in the polymer-binding process cost less than powders used in laser or electron beam melting processes, as the requirements on the former powder are less stringent. Systems such as the Markforged Metal X and Desktop Metal Studio have price tags on the order of $100,000. While still out of reach for many private consumers, they are certainly more accessible than laser- and electron beam-based systems that have current prices hovering above $500,000.

The cost of metal printing systems will continue to decrease. Yet, even before that happens, the accessibility of metal parts via service vendors raises similar potential security concerns. There are already many companies that own and operate metal 3D printers and market the ability to accept digital part files and turn around printed hardware. Such a business model further democratizes the access to printed metal parts. It is likely that such a service provider route could be pursued by an actor attempting to source metal parts for assembly into a weapon. Particularly if parts intended for an assembly are printed piecemeal, the intent or use of the parts may not be obvious and would not necessarily raise suspicion. The underlying presupposition is that metal parts—stronger and more durable than other types of 3D printed materials—could lead to a new

class of threats in terms of 3D printed weapons.

Proliferation of Safety Critical 3D Printed Parts

Timeframe: 0-5 years

As processes mature, print quality improves, and 3D printing technologies gain acceptance within mainstream manufacturing, the use of these techniques to produce safety-critical parts is likely to rise. Research in 3D printing is driven in large part by the aerospace, automotive, and medical industries. Within these industries, high-value parts justify development cost investments for 3D printed solutions. These solutions are driven by the desire to take advantage of 3D printing for ease of producing complex geometries, which could be optimized for material and weight savings and even individualized; for example, in the case of applications for prosthetics and biomedical devices within the medical industry.

Parts produced for critical applications in the healthcare and transportation industry are likely to have significant implications for public safety. As these industries adopt 3D printing, attack vectors based on vulnerabilities of 3D printing are a significant and growing concern.

Novel Materials

Timeframe: 2-7 years

The development of new materials for 3D printing goes together with the development of 3D printing machines and deposition processes. Advancements include the development of feedstock materials (both metals and polymers) tailored to printing processes to yield higher density parts with better mechanical properties and increased reliability. Material advancements also include development of novel materials that exhibit unique mechanical, thermal, optical, electrical, and magnetic attributes. These may include anisotropic properties (e.g. preferential electrical or thermal conduction in one direction). They may also include properties that are a function of tailoring material deposition at small scale, made possible by high-resolution, automated, multi-material 3D printing processes. These "engineered materials" pave the way for unique performance attributes of printed parts, which could include parts with very high strength-to-weight ratios, explosive materials, or high-strength plastics capable of withstanding pressures such as those encountered in a firearm.

3D-printed Chemical Formulations

Timeframe: 4-9 years

Use of 3D printing techniques to realize unique chemical formulations is an active area of research. A group from the University of Illinois - Urbana Champaign demonstrated an automated method for molecular synthesis of small organic molecules using a building block approach.[2] As this application area for 3D printing matures, potential use cases include pharmaceuticals with tailored time-release profiles or those tailored to a patient's unique physical characteristics. Furthermore, nefarious use cases could also include remote, undetectable manufacture of chemical and even biological weapons or poisons.

Multi-material Processes for Printing Embedded Electronics

[2] J. Li, S. Ballmer, E. Gillis, et al., "Synthesis of many different types of organic small molecules using one automated process," Science, 347 (2015): 1221-1226.

Timeframe: 5-10 years

Currently available multi-material printers allow for deposition of electrically conductive traces within a polymer matrix. With a trend toward improved resolution and new materials, the ability to print electronic components is within reach in the 2- 7-year timeframe. Researchers have experimented with printing capacitors, resistors, and inductors and demonstrated use of conductive polymer for a printed high-pass filter with properties comparable to a traditional filter.[3] 3D printing will also likely yield reliable energy storage solutions within the 5- to 10-year timeframe.[4]

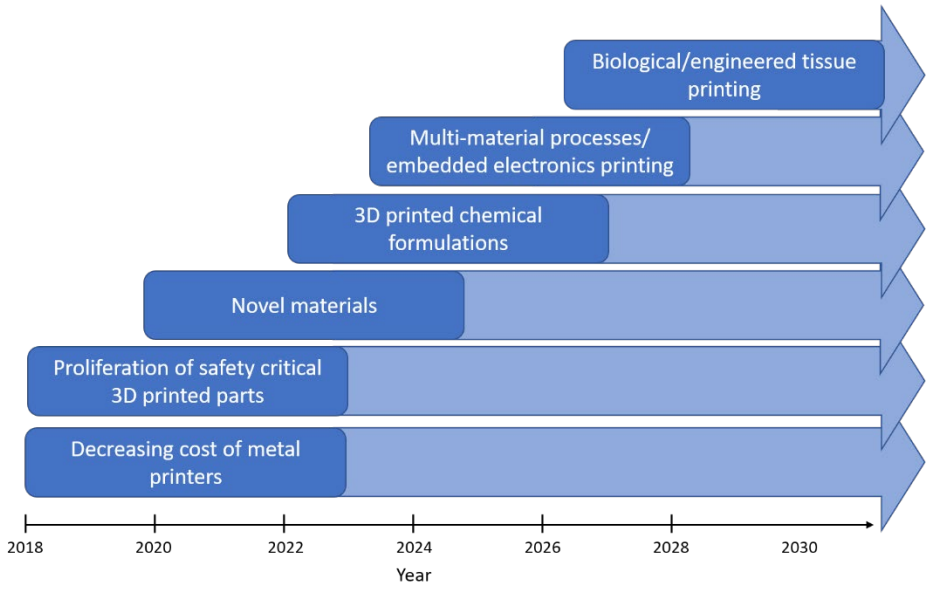
Biological/Engineered Tissue Printing

Timeframe: 10+ years

3D printing of cellular material, bio inks, and growth factors is being investigated to produce human tissue-like material and scaffolds. For engineered tissue, 3D printing offers the potential to address the needs for matching patient-specific anatomical data and producing complex features in three dimensions with high accuracy. The intersection of 3D printing with engineered tissue is one of the focus areas of the Advanced Regenerative Manufacturing Institute (ARMI), a public-private consortium opened in 2017 with the goal to "make practical the large-scale manufacturing of engineered tissues and tissue-related technologies."

1.3 Projected Timeline for Deployment of Future 3D Printing Advancements

Figure 6 illustrates a projected timeline for the advancements in 3D printing discussed above, all of which are likely to have an impact on Homeland Security.



[3] . Flowers, C. Reyes, S. Ye, et al., "3D printing electronic components and circuits with conductive thermoplastic filament," Additive Manufacturing, 18 (2017): 156-163.

[4] B. Yao, S. Chandrasekaran, J. Zhang, et al., "Efficient 3D Printed Pseudocapacitive Electrodes with Ultrahigh MnO2 Loading," Joule, (2018).

Figure 6: Projected Timeline for 3D Printing Technology Advancements

1.4 Impediments to Deployment of 3D Printing Technology

Catastrophic Failure of a Safety Critical Part

In 2015, General Electric obtained certification from the Federal Aviation Administration (FAA) for the first 3D printed part for use in a commercial jet engine. Use of 3D printed parts for aircraft was not new—they were already used for many non-critical parts like ducting and interior cabin parts—but this was the first part performing a function critical to flight to be certified by the FAA.[5] Flight critical, 3D printed parts have also been pursued within the Department of Defense (DoD). Naval Aviation Systems Command (NAVAIR) demonstrated flight of an aircraft containing 3D printed safety critical parts in July 2016.[6]

As 3D printing is increasingly used for production of safety critical parts, the risks associated with part failure grow. A hypothetical failure of a 3D printed part resulting in loss of life or serious economic impact could heavily influence public opinion and cripple implementation of 3D printing technologies for end use applications.

Foreign Manufacturers

Most 3D printing systems are supplied by foreign entities. Only approximately 21 percent of systems sold in 2017 came from manufacturers headquartered in the United States.[7] As such, advancements in 3D printing technology are likely to be affected by international trade policy as well as political and economic factors outside of U.S. control.

1.5 Convergence with Other Emerging Technologies

The convergence of 3D printing technologies with 3D scanning technologies allows for rapid generation of digital build files based on physical artifacts and subsequent reproduction of those artifacts. Potential threats exposed by the convergence of 3D scanning and printing include counterfeiting, biometrics spoofing, and intellectual property theft.

3D printing offers the ability to rapidly prototype hardware. As such, 3D printing functions as an enabler for other emerging technologies such as novel sensing and communications equipment. 3D printing as a rapid prototyping mechanism can lead to both capabilities for and threats to Homeland Security, as it will almost certainly accelerate the innovation curve for new technologies.

Convergence of 3D printing with other emerging technologies is highlighted in the section that follows.

2. How such technologies could endanger the homeland, with a focus on those which have the highest likelihood of becoming a threat and those that pose the highest consequences to U.S. homeland security.

2.1 New Capabilities for Homeland Security

[5] T. Kellner, "The FAA Cleared the First 3D Printed Part to Fly in a Commercial Jet Engine from GE," GE Reports, 14 April 2015, https://www.ge.com/reports/post/116402870270/the-faa-cleared-the-first-3d-printed-part-to-fly-2/.
[6] "NAVAIR marks first flight with 3-D printed, safety-critical parts," NAVAIR Press Release, 29 July 2016, http://www.navair.navy.mil/index.cfm?fuseaction=home.NAVAIR NewsStory&id=6323/.
[7] T. Wohlers, I. Campbell, O. Diegel, and J. Kowen, "Wohlers Report 2018," Wohlers Associates, Inc., March 2018.

Capability Use Case #1: Lightweight, Low-Cost Platforms for Intelligence, Surveillance and Reconnaissance (ISR)

3D printed assemblies can function as lightweight platforms for sensors to be used for ISR. The ability to print complex geometries, such as lattices, with relative ease enables high strength-to-weight parts that can allow for efficient airborne and ground-based platforms. Potential use scenarios for such platforms span from security to first responders. Ease of reconfiguration and customization of printed parts allows for such ISR platforms to be unique to the application and potentially easier to conceal as innocuous objects so as not to draw attention to them.

Capability Use Case #2: Supply Chain Risk Management

3D printing/additive manufacturing has the potential to mitigate supply chain risk for products critical to national security or economic stability. 3D printing technology enables the realization of complex geometries without the need for part-specific tooling that may be required for traditional fabrication. Moreover, the digital storage of parts data means that part fabrication routines can be sent digitally between geographically separated sites. As such, employing 3D printing for critical products allows for redundant fabrication capabilities and eliminates a "single-point-of-failure" scenario whereby a single manufacturing facility responsible for production of a critical part is taken offline halting the supply chain for that part. Moreover, 3D printing facilitates fabrication of parts closer to point of need/use, thereby overcoming shipping/transport obstacles that may arise in situations where infrastructure is limited due to either attack or natural disaster.

2.2 New Threats to Homeland Security

Threat Use Case #1: Sabotage of Safety Critical Parts

3D printed parts are susceptible to sabotage via the intentional, malicious modification of digital build files. Modifications can be carried out such that the part printed via the modified file appears to meet all requirements, while it actually contains concealed flaws or flaws so minute that they are not readily identified that result in premature failure. Such an attack vector was demonstrated by Belikovetsky et al. in an experiment called "dr0wned."[8] In this experiment, a digital file for an unmanned aerial system (UAS) propeller design was intentionally modified to remove a small amount of material in a critical structural region of the propeller. The propeller was thus designed to fail catastrophically, leading to its failure during a demonstration flight and subsequent downing of the UAS.

Threat Use Case #2: Concealment

Concealment refers to embedding of illicit objects within a 3D printed part, such that the printed part appears innocuous to the casual observer. Such threats may be carried out by pausing the 3D print, embedding or placing an illicit item within the build volume, and then resuming the print. The resulting 3D printed part may appear normal and legal, but conceals illicit objects such as explosives, illegal drugs, or embedded technologies for espionage (e.g. cameras, tracking devices, RFID chips).

Threat Use Case #3: Untraceable Weapons

[8] M. Belikovetsky, M. Yampolskiy, J. Toh and Y. Elovici, "Dr0wned cyber-physical attack with additive manufacturing," 11th USENIX Workshop on Offensive Technologies, Vancouver, BC, 2017.

Untraceable weapons include "ghost guns," named as such because they have no serial number, are not traceable, and are not detectable through metal detectors if 3D printed from polymer material.[9] Metal 3D printing may be employed to produce firearms or parts of firearms that are more durable than plastic equivalents and still avoid traceability.

Untraceable weapons may also include 3D printed explosives. The ability to print in multi-materials has led to research in the area of printed explosives by the DoD as well as academic groups.[10] Such explosives may be fabricated from constituent materials, which are widely available and do not raise concern until they are combined in a formulation to produce the explosive material.

Threat Use Case #4: Supply Chain Exposure

While distributed manufacturing enabled by 3D printing can be an opportunity for supply chain resilience, it also poses security challenges. Specifically, vulnerabilities exist with both the distributed printers themselves as well as with the digital part data.

Distributed 3D printing capability is vulnerable to malware and malicious interference. Weak points in the security of facilities housing 3D printers create potential opportunities for a malicious actor to interfere with production capability, either by rendering the printer inoperable or causing the printer to perform sub-optimally. The 3D printer may be meddled with via direct physical contact with the system, or it may be accessed remotely if the printer is networked.

With digital storage of parts data and build instructions come inherent cyber vulnerabilities; sensitive, proprietary, or critical design information may be exposed during the digital transfer of files between designers, engineers, and manufacturing technicians. Such attacks may be aimed at stealing data or, in a more sophisticated attack, replacing files in such a way as to cause failure of the 3D printer, failure of the build, or premature failure of the part produced (see, Threat Use Case #1: Sabotage of safety critical parts).

Threat Use Case #5: Counterfeits

As the cost of 3D printing systems is reduced, fabrication capabilities become more broadly accessible. Moreover, 3D printing service providers allow sourcing of custom parts for even lower costs as such avenues preclude investment in the printing system. Illicit use of 3D printed parts encouraged by accessibility include fabrication of credit card skimmers, weapons, weaponized UASs, banned products, and explosives.

3D scanning technologies can be used in conjunction with 3D printing systems to allow for ease of reproduction. An actor with physical access to a part may readily scan the part to produce digital design files in order to replicate high value goods, thereby infringing on copyrights and trademarks. Such use of 3D printing to produce counterfeits has economic impacts in terms of loss of market, jobs, and tax revenues and may lead to distribution of lower-quality and

[9] S. Grunewald, "What You Need to Know About 3D Printed Guns and Why You Don't Need to Fear Them," 3DPrint.com, 23 June 2016, https://3dprint.com/139537/3d-printed-guns/.

[10] H. Watkin, "Custom-Shaped Explosives for US Navy 3D Printed on HP 3D Printers," All3DP, 18 April 2018, https://all3dp.com/custom-shaped-explosives-us-navy-3d-printed-hp-3d-printers/.; S. Mraz, "3D Printing with Explosives," Machine Design, 11 January 2018, https://www. machinedesign.com/3d-printing/3d-printing-explosives/; and, J. Kerns, "A Look Inside the 'Explosive' 3D-Printing Industry," Machine Design, 26 February 2018, https://www.machinedesign.com/3d-printing/look-inside-explosive-3d-printing-industry/.

potentially dangerous products.

Threat Use Case #6: Biometrics Spoofing

The combination of 3D scanning and printing technologies has been demonstrated as a viable approach for spoofing biometrics. Such threats include fabrication of masks to spoof facial recognition software and prosthetics and fingerprints to spoof fingerprint readers. Attributes of 3D printing which lend it to such applications include:

- ease of individualization and customization of printed parts, and
- ability to produce gradient materials with varying mechanical properties from rigid to flexible

3. Recommendations to best mitigate the perceived deleterious impacts of the assessed technological advancements, including recommended DHS near and long-term actions. Provide an assessment on the perceived opportunities for DHS components to maximize the use of these new technological advancements to guard against emerging threats

Recommendation #1: Technologies for integrated "Attribution" for AM Printers

The ability to embed information within 3D printed parts can serve as the basis for traceability of parts to the originating machines and build files. The proposed approach is analogous to methods incorporated by document printer manufacturers for embedding data within printed documents produced on laser printers.[11] Such technologies do not currently exist for 3D printers. Traceability of 3D printed parts to source machines and source files can benefit commercial entities (IP protection), end users (counterfeit detection), and law enforcement (deterrence and prosecution) in mitigating threats posed by 3D printing technology.

Blockchain—a distributed, decentralized, public ledger that encrypts, validates, and permanently records transactions—is complementary to the ability to embed information in 3D printed parts. Blockchain ledgers are well suited to tracking 3D printed parts in a distributed manufacturing environment. They allow for multiple authorized parties to update a distributed, public ledger. A unique tag embedded in a 3D printed part can be used to trace the history of that part from the time it is fabricated to the time it reaches the end-user. Such an approach to using blockchain was presented for improving the security of 3D printed parts using fluorescent nanoparticle-based tags.[12] A filament doped with fluorescent nanoparticles was used to deposit a public key (a QR code) within a 3D printed part based on asymmetric cryptography, while the emission profile from the nanoparticles served as the private key. The QR code provided a link to a blockchain ledger so that at each point in the 3D printed part's chain of custody, the QR code could be scanned and the part's digital ledger amended.

Recommendation #2: Enhanced Detection Mechanisms

Enhanced imaging and detection tools can aid in countering concealment threats. Capabilities

[11] J. van Beusekom, F. Shafait, and T. Breuel, "Automatic authentication of color laser print-outs using machine identification codes," Pattern Analysis and Applications, 16 (2013): 663-678.

[12] Z. Kennedy, D. Stephenson, J. Christ, et. al., "Enhanced anti-counterfeiting measures for AM: coupling lanthanide nanomaterial chemical signatures with blockchain technology," Journal of Materials Chemistry C, 5 (2017): 9570-9578.

needed include:

- rapid through-part imaging to identify objects concealed within printed parts that otherwise appear innocuous,
- high resolution through-part imaging to identify flaws intentionally embedded in critical parts that may lead to premature part failure, and
- detection of printed explosives material.

Recommendation #3: Reinforced Cybersecurity Measures

An important attribute of 3D printing is the ability to rapidly share design data, 3D models, and manufacturing (build process) files across networks with multiple users and systems. Digital data is readily shared between designers and engineers as well as manufacturing technicians and 3D printers, enabling rapid, iterative product development. To support this workflow, robust means for protecting digital data that may include sensitive, proprietary, or critical design information are needed. Such cybersecurity measures taken to protect digital data should be routinely monitored to ensure they address evolving attack vectors and cyberthreats.

This page is intentionally left blank.