HSOAC HOMELAND SECURITY
OPERATIONAL ANALYSIS CENTER
An FFRDC operated by the RAND Corporation under contract with DHS

RESEARCH REPORT

DANIEL M. GERSTEIN, ERIN N. LEIDY

EMERGING TECHNOLOGY AND RISK ANALYSIS

Additive Manufacturing

Additive manufacturing (AM) or three-dimensional (3D) printing—which is a subset of the broader advanced manufacturing revolution—has reached a level of technological maturity, accessibility, and availability in the past decade that contributes to an exponentially increasing proliferation of the technology across a wide variety of licit and illicit use cases. This growth has been fueled by complementary technology advancements in materials science, computer-aided design, and artificial intelligence (AI), to name a few. The fact that more 3D printing materials and techniques are available has contributed to more sophisticated use cases.

Although AM technology has been maturing for more than four decades, the 2013 printing of a 3D printed gun brought the issue to the forefront and illustrated the potential for illicit use cases that could threaten national security. The distributed nature of 3D printing allows development of made-for-purpose technologies to support a wide variety of uses. It facilitates decentralized manufacturing, rapid prototyping, and proliferation of basic designs that can be tailored to meet user specifications. These user specifications can include "violent actors [who] might be able to replicate more sophisticated weapons systems, print lethal drones, and even produce jamming devices or cheap decoys that disrupt intelligence collection."[1]

The lower costs and growing availability of "manufacturing hardware (printers), raw materials and software (intellectual property [IP])" will lead to a growing use of 3D printing as a replacement for traditional manufacturing uses, as well as for illicit purposes.[2] AM—which will lead to order-on-demand manufacturing—will also affect supply chains, potentially making them less global and more localized. These changes will create new challenges in countering the proliferation of potentially dangerous products and technologies because the focus will likely need to change from interdicting end products and physical technologies to software and IP. Regulatory and export control regimes will likely also be affected as attempts are made to stop the proliferation of computer-aided designs for products and counterfeits, as well as subpar products that could affect consumer safety.

We assessed that attempts to limit the proliferation of printers will also likely be challenging because greater use of 3D printing for legitimate commercial uses should be expected to continue. 3D printed components, some with untested and unknown failure rates, will likely be incorporated into end products, which could result in catastrophic failures. Although AM has numerous applications, including aiding in the manufacture of advanced and untraceable weapons, in this review, we focused on the commercial use of AM and the risk posed by counterfeiting due to the less visible but significant impacts this could have on economic prosperity and national security.

KEY FINDINGS

- Advances in additive manufacturing (AM) or three-dimensional (3D) printing will continue, thereby increasing the use of this capability for a wider variety of licit and illicit activities. Advances in AM will be fueled by scientific discovery and technology development in converging technologies, such as artificial intelligence (AI), materials sciences, biology, chemistry, and nanotechnology.
- Counterfeit 3D printed materials and products will present new threats, vulnerabilities, and consequences, including implications for security, product safety, considerations for the economy and IP rights, the convergence of technologies, and the printing of illicit or banned products.
- Items produced through AM as counterfeits are unlikely to be subjected to the same necessary policy, legal, ethical, and regulatory provisions as licit goods. Although illicit products could be developed that look, feel, and even function like their strictly regulated counterparts, they could have vastly different life spans and failure modes.
- The AM revenue projection for 2030 is expected to grow annually between 2022 and 2030 by 24.3 percent, to $105 billion. However, this projection is dwarfed by the 2022 global manufacturing production total of $44.5 trillion. Still, AM will likely play an outsized role in several key sectors, including health care, aerospace, education, manufacturing (in specific areas, such as rapid prototyping, printing replacement parts, and custom solutions), automotive, and robotics.
- Despite the potential for high-consequence incidents with 3D printed counterfeits during the ten-year time horizon of the study, we assessed that these were likely to be more locally confined and unlikely to result in widespread events, which placed them in the moderate technology risk category.

In our analysis, we considered four attributes in assessing AM technology: technology availability (T_{AV}) and risks and scenarios (R_S), the latter of which we divided into threats, vulnerabilities, and consequences. The R_S considered in this analysis pertain to the impacts of the counterfeiting of technologies. We examined a wide variety of negative effects associated with the counterfeiting of technologies for 3D printing. The R_S have been provided by the study sponsors in the U.S. Department of Homeland Security (DHS) Science and Technology Directorate and Office of Policy. We compared these four attributes across three periods (see Figure 1).

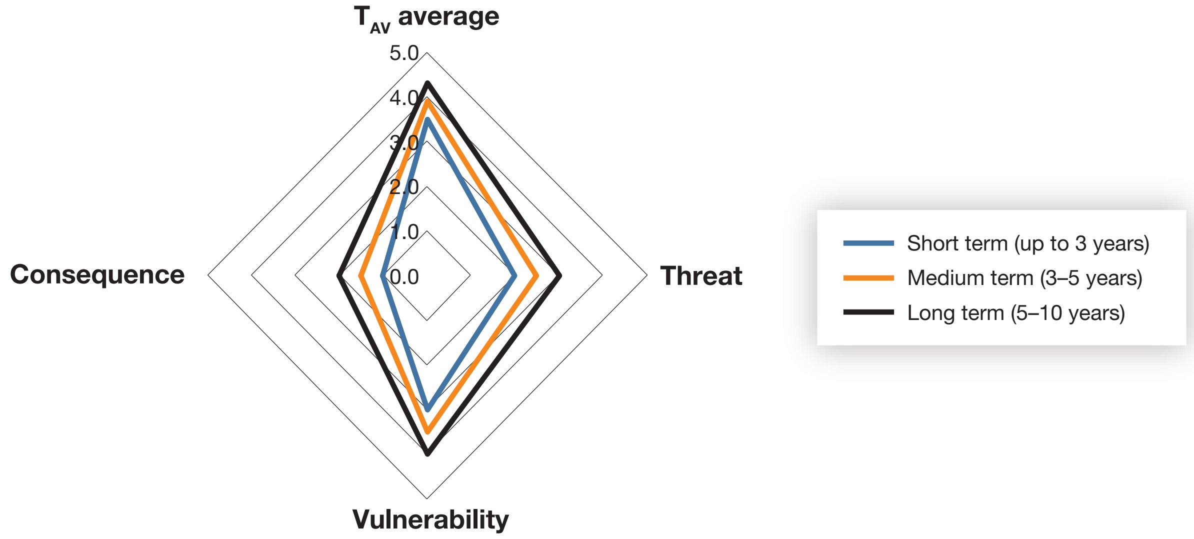
Overall, we assessed that the technology will continue to mature over the ten-year horizon of the analysis. The number of threat actors with access to these capabilities is likely to grow as the technology proliferates. However, for the vulnerability assessment, we determined that anticounterfeiting measures that are in development, such as tagging and tracking, will likely come to fruition by the end of the study period—the result will be a lowering of the overall vulnerability resulting from AM for some use cases (including the counterfeiting of goods). Despite the potential for high-consequence incidents with 3D printed counterfeits during the ten-year time horizon of the study, we assessed that these incidents were likely to be more locally confined and unlikely to result in widespread events, which places them in the moderate consequence category. These assessments are likely to change over a longer time horizon. As a *Financial Times* article states, “[a]t current growth rates, half of all manufactured goods will be printed in 40 years.”[3] Should such adoption of AM occur, the risks are likely to rise precipitously as well.

TECHNOLOGY DESCRIPTION AND SCENARIOS FOR CONSIDERATION

According to defined standard terminology, *AM* is “a process of joining materials to make objects from 3-D model data, usually layer upon layer, as opposed to subtractive methodologies. Synonyms for Additive Manufacturing include additive fabrication, additive processes, additive techniques, additive layer manufacturing, layer manufacturing, and freeform fabrication.”[4] All AM uses 3D printing to create new objects; in practice, the terms can be used interchangeably. The primary classes of materials that are used in AM today are metals, plastics, and ceramics, although it is feasible to print using numerous

FIGURE 1

ADDITIVE MANUFACTURING RISK ASSESSMENT



NOTE: The emerging technology risk assessment scale is 0 to < 2 = low impact or not likely feasible, 2 to < 4 = moderate impact or possible, and 4 to 5 = high impact or likely feasible.

other materials.[5] AM is often discussed in terms of seven basic categories: binder jetting, directed energy deposition, material extrusion, material jetting, power bed fusion, sheet lamination, and vat photopolymerization.[6] The differences between these techniques is not important for this report; what they have in common is that each provides a method for building objects in which material is deposited one layer at a time.

AM was introduced in the 1980s, building from a foundation of research to the 1987 release onto the market of the first commercial device for 3D printing.[7] Important benefits associated with AM are "producing goods at an extraordinary speed, using less material, and reducing labor costs."[8] New processes were developed throughout the 1990s. The technology has continued to build on these foundations, and a wide variety of materials have now become available for use in 3D printing. Many commercial industries now find important benefits associated with AM over traditional manufacturing: It allows rapid prototyping of new designs; a decrease in waste; small-batch production; and the design of products that can be stronger, weigh less, or have other advantages over traditionally manufactured parts. AM has seen uneven adoption across commercial sectors, but, in some industries, including aerospace, construction, medicine, energy, and consumer goods manufacturing, adoption of AM is spreading. Additionally, 3D printers have become affordable for personal, in-home use; many can be found for less than $500.

METHODOLOGY

We developed a framework for assessing the risks of emerging technologies. The assessment included an evaluation of the T_{AV} and potential R_S for which a technology could be used. The T_{AV} evaluation covered five areas: science and technology maturity; use case, demand, and market forces; resources committed; policy, legal, ethical, and regulatory impediments; and technology accessibility.[9] The R_S evaluation covered threat, vulnerability, and consequence. The ratings for the T_{AV} and R_S categories ranged from 1 to 5, where 1 corresponds to many challenges and 5 to very few, if any, challenges. The five T_{AV} areas were averaged and included in the emerging technology risk assessment. To allow the comparison of emerging technologies in our assessment of the consequences, we rated impacts according to the likely affected level (national, regional, or local), potential mortality and morbidity, and likely economic and societal disruption. By averaging the threat, vulnerability, consequence, and T_{AV} average calculated previously, an emerging technology risk for a particular scenario could be assessed as low (0 < 2), moderate (2 < 4), or high (4 to 5).

These assessments were repeated for three periods: short term (up to three years), medium term (three to five years), and long term (five to ten years). This allowed us to assess individually and collectively how T_{AV} and R_S would be affected over time. In the assessment, we considered how the threats, vulnerabilities, and consequences evolved over time, as well as whether any preparedness, mitigation, and response activities had been undertaken that could reduce the risk.

THE TECHNOLOGY AVAILABILITY ASSESSMENT

The T_{AV} assessment was conducted without regard to the specific R_S. Those factors are addressed in the subsequent discussion of the R_S assessment. We separated these assessments in this way to isolate the effects of the changes in technology over the ten-year study time frame.

An interesting point of departure in this T_{AV} assessment comes from highlighting the advantages and challenges of AM. The Welding Institute, an industrial, membership-based organization, provides a list of advantages of 3D printing: flexible design, rapid prototyping, printing on demand, strong and lightweight parts, fast design and production, minimization of waste, cost-effectiveness, ease of access, environmental friendliness, and the enabling of advanced health care. The institute's list of disadvantages consists of the fact that materials for printing are limited, build sizes are restricted, there are requirements for postprocessing, large volumes do not benefit from economies of scale the way injection molding does, structures can delaminate, the number of manufacturing jobs decreases, design inaccuracies can be introduced, and copyright issues can arise.[10]

We did not delve deeply into the specifics of different types of AM processes. These processes continue to evolve over time in terms of both their efficiency and the types of materials and applications that are becoming available. As we discuss later in this report, early 3D printing applications were small and limited in terms of materials. More recently, the scale has greatly increased to include the 3D printing of houses and rockets and employing a wider array of materials.

SCIENCE AND TECHNOLOGY MATURITY

In 1987, the stereolithography printer was developed. It used lasers to cure a liquid resin into a hardened plastic in a process called *photopolymerization*.[11] This process or one very similar has been used in multiple generations of 3D printing equipment. An example of this progression is selective laser sintering, which uses a high-power laser to sinter, or melt, "small particles of polymer powder into a solid structure."[12] Subsequent 3D printers have employed a wider variety of materials, increased printing speeds, reduced costs, and eliminated waste.

The use cases for 3D printers have progressed as well, from research to rapid prototyping and small niche applications to larger structural prototypes and parts. These printers enable their users to print for a multitude of purposes, both licit and illicit. Small 3D printers are on the market right now for home use, which allow users to print small items, including unregistered weapons and false biometrics, such as fraudulent fingerprints.[13] Larger 3D printers are being used in many industries. For example, the aerospace industry was an early adopter of this technology; such a capability would likely be essential for a future crewed mission to Mars—specifically, providing the ability to make "tools or rocket parts" while on the planet.[14] Another example of large commercial-scale 3D printing applications can be seen at the Oak Ridge National Laboratory facility, where researchers are "refining their design of a 3-D-printed nuclear reactor core, scaling up the additive manufacturing process necessary to build it, and developing methods to confirm the consistency and reliability of its printed components."[15] The goal of this effort is to have a 3D printed reactor by the end of 2023. In another Oak Ridge National Laboratory program, a large-scale thermoset 3D printer has been installed that can work with "previously unworkable materials," such as plastics that will be "irreversibly cured."[16]

The industry continues to expand, enabling the printing of larger systems with greater complexity. In 2023, the startup Relativity Space launched the "world's first 3-D-printed rocket," the Terran 1, which was a 110-foot-tall space launch vehicle designed to carry lightweight satellites into orbital space. Because its engine failed, the rocket did not reach orbit, but no issues related to the rocket's structure were encountered.[17]

With applications for constructing homes, office buildings, and other structures, 3D printing has also found its way into the construction industry; one account offers that "3D-printed buildings can span thousands of square feet and multiple stories and are more affordable than traditional construction methods. For civil engineers, polymer 3D printing offers a way to quickly produce prototypes of bridges, roads, and other structures."[18] Another source identifies such applications as a potential solution to affordable housing and a way to make space habitable for human beings.[19]

Early 3D printing applications were small and limited in terms of materials. More recently, the scale has greatly increased to include the 3D printing of houses and rockets and to employ a wide array of materials.

In addition, 3D printing has been demonstrated for precise applications at the nanoscale level. For example, 3D printed nanomaterials and nanotechnology-enabled final products are being used for patient-specific biomedical equipment and for use in dental applications and neurosurgery.[20]

Identifying a technology readiness level (TRL) or maturity for 3D printing is challenging. We assessed that the basic technology and concepts for 3D printing were well understood and in use, meaning that they are at a high TRL. Furthermore, as use cases continue to be identified, new materials are being developed for use in 3D printing and new methods for printing (such as those employing large-scale gantries like those used in the construction industry) are developed. Undoubtedly, the technology and applications will continue to mature and will continue to be fueled by the convergence of other technologies, such as AI. Still, they would be based largely on the basic technology and concepts from earlier 3D printing applications. In addition, four-dimensional (4D) printing is on the horizon. Four-dimensional printing entails 3D printed objects that have the ability to “change or transform over time, without human interaction.”[21] In 4D printing, materials—such as nanomaterials—could self-assemble and even decompose to allow the materials to be reused. Applications for 4D printing include use in extreme environments, such as space, where it would be useful to have “self-configuring materials,” or even in biomaterials that might need to evolve over time.[22]

USE CASE, DEMAND, AND MARKET FORCES

From the beginning of its development in the 1980s with no market share to a global market worth more than $4 billion in 2014 and an expected market of more than $105 billion by 2030,[23] AM has experienced rapid growth and is expected to continue to do so during the study time frame.

AM, combined with other emerging technologies, including data analytics, AI, predictive manufacturing, and materials science, is expected to have vast repercussions for the state of global and U.S. manufacturing. As things become easier to produce with these methods, not as large a footprint or workforce is required, leading to a potential loss of jobs in numerous industries. Pieces of the global supply chain are also at risk; if parts can more effectively be manufactured close to where they are needed, the need to source parts halfway around the globe lessens.

3D printing can reduce costs and opportunities for designing specific characteristics into additively manufactured products. It also offers such features as print on demand, can reduce inventory holding costs associated with traditional manufacturing, and reduces dependence on supply chains. Such products can be designed and delivered to meet certain specifications employing a variety of materials that best suit the envisioned applications.[24] The use of 3D printing for prototypes and toolmaking is particularly attractive because such products can be rapidly assembled, tested, used, and even recycled for one-time-use applications. The incorporation of AI capabilities, including machine learning, has the potential to further improve product performance (e.g., monitoring the manufacturing process to fix printing errors in real time).[25]

However, factors exist that restrain AM from being incorporated across many industries. Take, for example, the aerospace industry, which has embraced 3D printing for prototyping (78 percent of companies) but has limited its use in end-part manufacturing (18 percent of companies).[26] Although many parts can be 3D printed, many others cannot be—the list of materials that can be used in 3D printing is limited by such considerations as temperature and safety. Postprocessing is another concern: Many 3D printed components require sanding, further molding, and other processes that introduce a time-consuming step into the manufacturing process.[27]

3D printing allows rapid prototyping, software stress-testing, in-house tooling, savings in weight and materials, and low development costs.

Additionally, quality standards for critical parts have, at times, proven difficult to meet or are lacking for this manufacturing method.[28]

Despite these limitations, the 3D printing of drones demonstrates why the proliferation of the technology is likely to continue. It allows rapid prototyping, software stress-testing, in-house tooling, savings in weight and materials, and low development costs.[29] These advantages not only mean faster progression from concept to prototype to technology fielding but also offer greater advantages in the effectiveness and efficiency of the 3D printed object, such as a drone. Reducing the weight of a drone airframe increases both the system's capacity to carry mission packages and other operational capabilities.

These benefits scale to the development of full-sized aircraft as well. Boeing's T-7A Red Hawk was digitally designed with many of the parts employing 3D printing and advanced manufacturing techniques. Thanks to these methods, the jet was "developed from concept to first flight in 36 months."[30] Development of the T-7A used "model-based engineering, 3-D tools and other advanced manufacturing techniques [which] enabled Boeing to forgo drilling on the T-7 production line, allowing the company to reduce incidents involving foreign object debris and enhance the quality of its build."[31]

RESOURCES COMMITTED

As with other technologies as they move from research to early adopters to widespread use, the costs associated with procuring and using technologies continue to decrease. Early personal 3D desktop printers cost $50,000 and had little capability compared with today's $500 variants that often can print with a wider variety of materials more efficiently.[32]

Relatively inexpensive desktop 3D printers are available and well within the reach of hobbyists, schools, do-it-yourselfers, start-ups, fabrication labs, and mobile machine shops. 3D printers that were more capable—likely for use in labs and research and in prototyping—are attractive for industry, academia, national labs, and government agencies. High-end production for use in the aerospace, medical, and automotive industries; jewelry; printing services; mold-making; and tooling for a variety of commercial applications has also become more widely available. The cost of these different platforms is also scalable, from very affordable at the desktop machine level at several hundred dollars up to several hundred thousand dollars for commercial applications.[33]

We assessed that the growing infusion of resources to develop new 3D printers employing a wider variety of materials more effectively and efficiently will result in the printers becoming more affordable while providing greater capabilities.

As new materials are integrated into 3D printing, additional use cases and market share are also likely to increase. One account offers that the "global 3-D printing market will reach $105,407.5 million by 2030, growing by 24.3% annually over 2022–2030."[34]

POLICY, LEGAL, ETHICAL, AND REGULATORY IMPEDIMENTS

Additively manufactured products are largely untraceable with today's protocols and capabilities and are thus able to avoid current regulations. Examples are 3D printed firearms, which have advanced in capability from designs that shot one bullet and fell apart to semiautomatic rifles that can shoot thousands of rounds.[35] No specialized technical knowledge is necessary to make these devices—just instructions downloaded from the internet and a relatively low-cost 3D printer. The weapons are printed without serial numbers and with no way for authorities and regulators to know their points of origin. Furthermore, at present, manufacturing a gun for personal use is legal; it falls under the same category as guns that are assembled from kits for personal use. Manufacturing a gun with the intent to sell or distribute it requires that the dealer follow standard gun regulations, such as adding serial numbers and running background checks before purchase.[36] Such nuanced specifications are challenging to enforce.

The International Traffic in Arms Regulations is in place to restrict the export of defense- or military-related technologies from the United States.[37] Guns that are 3D printed are exempt from these regulations; they fall under Export Administration Regulations instead.[38] The International Traffic in Arms Regulations still applies to many other defense-related 3D printing technologies and digital instruction files because it regulates "information for the design, development, manufacturing of defense articles, including blueprints, drawings, documentation, etc."[39] However, digital information can be extremely difficult to control. Once released, restricting who has access to that information is difficult. For example, the U.S. Department of Commerce's Bureau of Industry and Security recently released information in a proposed charging letter that alleged that 3D Systems Corporation committed 19 violations of the Export Administration Regulations "by exporting controlled aerospace technology and metal alloy powder to China without the required license, and by exporting controlled technology to Germany without the required license."[40]

AM also poses challenges to IP law, in which the center of gravity for IP enforcement actions can go from the physical product to software and computer-aided design files. In this IP enforcement, borders do not have the same importance: Limiting the physical movement of goods becomes less relevant than controlling the virtual proliferation of IP. Current legal protections for AM IP rely largely on existing patent law, which can fail to fully protect owners of digital IP.[41] However, given the continued use of traditional manufacturing and the growing use of AM, both regulatory regimes will be necessary.

Highlighting the extent to which 3D printing could change access to sensitive materials, as well as altering supply chains, one *RAND Blog* post highlights 3D printing's potential to leapfrog borders, sanctions, and tariffs.[42] This post also highlights one trade analyst's prediction that "3D printing could wipe out almost a quarter of cross-border trade by 2060."[43] Whether global manufacturing and supply chains will be so dramatically affected remains an open question, but such a claim highlights the growing potential for 3D printing to alter international relations and trade between nations.

Additionally, individual industries are regulated by different guidelines for product safety, such as those of the U.S. Food and Drug Administration for medical implants and devices and those of the Federal Aviation Administration for airplane parts. In such cases, quality and consistency are required in the end product and in regulatory manufacturing processes. Failure to achieve this consistency could result in substandard and potentially dangerous products.[44]

Finally, products created as counterfeits are not likely to be subjected to the same policy, legal, ethical, and regulatory provisions as licit goods are. Illicit products could be developed that look, feel, and even perform like their strictly regulated counterparts but have vastly different life spans and failure modes. More on this subject is covered in "The Risk Assessment" later in this report.

TECHNOLOGY ACCESSIBILITY

As previously mentioned, 3D printers have lowered in price to a point of affordability for home use. Instructions for 3D printing guns are freely available on the internet, and manufacturing one takes no special skills. We assessed that users will likely see 3D printer prices and materials also become more available while providing greater access to a wide array of applications, including large-scale commercial activities (such as 3D printed rockets) and the printing of biomaterials and explosives.[45]

Although companies are likely to attempt to "control" or manage access to sensitive materials, such as instructions for making dangerous weapons or unique repair parts, doing so will prove challenging because, via hacking or other cybersecurity risks, digital instructions are likely to proliferate and limiting access becomes more challenging once that occurs. The wider variety of materials available for 3D printing applications will allow more use cases to be envisioned.

Although we assessed that 3D printing was becoming readily accessible, larger-scale printers that are more advanced will likely be more challenging to access than smaller ones, which individuals are buying with no restrictions. This availability will extend to individuals seeking to use the applications for illicit purposes. As a result, 3D printing makes other technologies and devices that are difficult to obtain—such as advanced weapons, explosive materials and devices, or other national security technologies—more accessible to illicit actors, including terrorists and criminals, to manufacture on their own.

OVERALL TECHNOLOGY AVAILABILITY

In addressing T_{AV}, we assessed that few impediments exist today or out to the end of the study time horizon that would prevent the continued proliferation of 3D printing. Furthermore, we assessed that AM will augment and, in some cases, replace the traditional manufacturing field for an increasing number of specialized products and technologies, as well as potentially for the illicit use of 3D printed capabilities. More on illicit uses is covered in "The Risk Assessment" later in this report.

Table 1 provides our assessment of the potential for 3D printing T_{AV} in the short term, medium term, and long term. Our findings from this T_{AV} assessment do not necessarily indicate that the technology will be used for illicit purposes—this possibility is addressed in the R_S discussion. However, they do indicate that T_{AV} barriers have been considerably lowered and that the potential for employing 3D printing capabilities for illicit purposes will become a growing possibility.

According to our evaluation of the individual T_{AV} categories, **science and technology maturity** and **use case, demand, and market forces** will continue to increase, and the technology will become more readily available over the ten-year study time frame. Few limitations exist today, and even fewer will exist in the future as the technology continues to expand, both in terms of materials available for use in 3D printing applications and in terms of the use cases that continue to be discovered. For most applications, 3D printing is already at a high TRL. Only 3D printing with specialized materials (e.g., for organs and certain parts subjected to high temperatures and stresses) should not be considered mature technologies.

Neither **resource** constraints nor **policy, legal, ethical, and regulatory impediments** will present significant barriers to the employment of 3D printing capabilities. In fact, the growing number of use cases, ubiquity of the technology that we expect to continue, that relatively few impediments could limit proliferation, and that relatively few unique parts are required for 3D printers will contribute to a rapid expansion in these capabilities that will go largely unchecked.

Given the ratings for the other four elements of T_{AV}, we assessed that the final category of **technology accessibility** will go from moderate to high by the medium term and remain so through the end of the ten-year period under consideration. Furthermore, we assessed that 3D printing was already a mature technology and will continue to see “life-cycle enhancements” in the form of better printers that are more efficient, the inclusion of new materials for specific purposes, and increased availability. One should expect that such life-cycle improvements will continue, making this technology readily available for a variety of threat actors. We discuss this risk in more detail in the next section.

THE RISK ASSESSMENT

Our risk assessment focused on the threats, vulnerabilities, and consequences of counterfeiting products and technologies developed using AM.[46] It built on the T_{AV} evaluation, from which we concluded that the risk specific to this scenario—that of counterfeited products being made using AM—already exists. However, as AM technology proliferates, the share of goods that are counterfeit will likely continue to rise, as will the risks associated with these counterfeited goods.

Our focus in this analysis was on the counterfeiting of 3D printed materials and products, which could result in a wide variety of threats, vulnerabilities, and consequences, including implications for product safety, the economy, IP issues, convergence of technologies, and the printing of illicit or banned products. Furthermore, we assessed that advances in AM will continue to be fueled by scientific discovery and technology development in AI, materials sciences, biology, chemistry, and nanotechnology, to name a few.

THREAT

A wide variety of actors with an equally wide array of motivations will have increasing access to AM capabilities, with an increasing ability to print larger quantities

TABLE 1

ADDITIVE MANUFACTURING TECHNOLOGY AVAILABILITY

Scenario	Science and Technology Maturity	Use Case, Demand, and Market Forces	Resources Committed	Policy, Legal, Ethical, and Regulatory Impediments	Technology Accessibility	T_{AV} Average
Short term (up to 3 years)	3.5	3	3.5	4	3.5	3.5
Medium term (3–5 years)	4	3.5	4	4	4	3.9
Long term (5–10 years)	4.5	4.5	4.5	4	4	4.3

NOTE: The emerging technology risk assessment scale is 0 to < 2 = low impact or not likely feasible, 2 to < 4 = moderate impact or possible, and 4 to 5 = high impact or likely feasible.

of sophisticated products. The threats will come from foreign and domestic sources and include a multitude of actors—foreign governments, terrorist groups, criminal organizations, and lone wolves. However, the threat actors alone do not determine the variety of vulnerabilities. These threats can be either deliberate or inadvertent in the case of substandard products that are being illegally sold.

State actors could be involved in commercial counterfeiting, especially in the case of state-sponsored commercial industry. Terrorist organizations are less likely to use AM for commercial purposes but could use AM to create materials and products to further their interests. Criminal organizations will likely employ AM to further their economic interests and to profit from stolen IP. Even individuals are likely to gain access to and use 3D printing illicitly, although these use cases are less likely to result in widespread vulnerabilities and consequences. An example is a home 3D printer being used to print a replacement part for a refrigerator door.

Safety and national security threats can also occur from actors without the intent to cause harm, either from counterfeiters or from legitimate manufacturers. Dispersed AM multiplies the number of actors in a supply chain, which complicates the regulation and quality control of the products or technologies. In some cases, in which such products are printed offshore, the distribution and entry into the United States of 3D printed counterfeited products might require an organized network (or supply chain).

Although threats could come from a variety of actors, we assessed that the severest and most-pervasive threats will come from commercial entities or organized criminal groups. Such threat actors could use AM to 3D print illicit goods, both simple products (some which could even be printed by an individual) and products that are more advanced, given the resources and access to proper machinery. Depending on the location, these actors could be commercial entities or organized criminal groups.

As the technology becomes more readily available and more powerful, additional use cases across a wider array of fields and specialty areas will likely emerge. For example, 3D printed drones are in use in the Russia–Ukraine War. Ukraine has employed AM for developing suicide drones;[47] the Russians have developed a similar capability.[48] The demonstrated benefit has been the rapid development and fielding of custom-printed products for highly specific purposes.

The positive projections for the industry and the potential for achieving improved performance characteristics highlight that the technology is likely to proliferate and therefore will be available to an increasing number of threat actors. For example, a July 2023 assessment highlights six industries that 3D printing is transforming: health care, aerospace, education, manufacturing, automotive, and robotics.[49] Although these industries might be leading in AM applications, other industries are also moving to acquire these capabilities. In March 2023, a 110-foot-tall and 7.5-foot-wide 3D printed rocket "made entirely from 3D-printed parts" was launched from Cape Canaveral Space Force Station in Florida. The 3D printed engines used a combination of copper, chromium, and niobium that allowed them to tolerate temperatures 40-percent higher than traditional copper alloys could.[50] This demonstrated both the increased speed to develop and manufacture such a system and the increased performance characteristics that are possible using AM.

With these growing use cases and scenarios, AM will likely continue to expand rapidly and find other areas that would benefit from these unique engineering capabilities. The 24.3-percent annual projected growth rate from 2022 to 2030 indicates the market's growing potential. This growth also suggests a continued proliferation of the technology and more actors having access to the technology.

VULNERABILITY

Although counterfeiting can be accomplished in many industries and using many technologies, AM poses a unique risk because of the ease of additively manufacturing products, the availability of the necessary manufacturing tools (3D printers), and the associated cybersecurity risks posed by digital plans for 3D printed products.

We assessed that the simpler the product, the more vulnerable it is to counterfeiting. Most threat actors could probably replicate a small product printed using readily available plastic material. On the other hand, we assessed that larger products using advanced or even composite materials will require specialty machines for manufacturing that might not be as available for individual actors but will likely be available to businesses or states. Additionally, we assessed that, as use of AM grows, new categories of counterfeits will likely be identified.

Counterfeits could be created in a variety of ways, such as hacking printing instructions from the licensed manufacturer, reverse-engineering a product using 3D scanning, or modifying 3D printing instructions to develop a "new" product. Each poses a threat to a company's IP rights if the company has exclusive rights to manufacture a certain item. Breaches in cybersecurity could also result in the hacking and adulteration of printing instructions, which could result in defective products reaching the market, albeit from legitimate and even trusted sources, including incidences of corporate sabotage.

Consumer safety is also potentially at risk with these products, particularly if the product is intended for use in a critical industry, such as health care or aerospace; the counterfeiter might be creating an inferior product, using different material, or using an incorrectly calibrated printer. Alternatively, the counterfeiter could introduce variations in the design that pose a risk to safety. Consider a medical device scenario from health care in which a 3D printed structure was embedded in a patient and the material or the adhesive between the layers leached into the patient's bloodstream, causing serious illness or death. In each of these cases, the counterfeit product might be visually indistinguishable from the original, including the use of company brand markings, making detection extremely difficult and posing risks to company reputation and liability in the event of a deficiency.[51]

During the 3D manufacturing process, concerns can arise that could result in safety issues and lower-quality products. Some of these issues relate to the quality of the equipment a counterfeiter might be using or to equipment that is out of tolerance. Examples of problems that can occur during 3D printing are warping, which can be a result of the lack of adhesion to the printer bed or thermal contraction of the upper layers; cracking, which can be the result of poor adhesion between layers and thermal shrinkage based on the temperature differentials of different sections of the printed object; and layer shift, which can be a result of excessive temperature in the motors or drivers, lack of power in the motors, or a mechanical failure.[52] The results can be different and unpredictable failure modes or 3D printed technologies that do not perform adequately.

The vulnerability of the 3D printed products also stems from not having proper regulatory oversight of decentralized 3D printing manufacturing processes. As new equipment (e.g., a new printer) is employed, new materials used for printing products, and perhaps even purported upgrades to the existing (and approved) design are made, counterfeiters would not likely subject these modifications to any sort of approval process or licensure. In contrast, the licensed manufacturer would be required to gain approval for major modifications from the regulatory body that governs this product. This vulnerability could be particularly troubling to regulate, depending on which federal entities have regulatory authority over the product or the technology—in many cases, several departments and agencies would.

AM introduces vulnerabilities into the current IP system, which could significantly affect corporate investments in research, development, and innovation, making the investment of funds in these activities less attractive for industry and entrepreneurs. AM also raises such questions as, "What types of changes to a product or technology would be required for it to be considered a new product?" This issue has important implications for protecting IP rights.

Although it is not directly related to the counterfeiting scenarios discussed previously, 3D printing of energetic materials (i.e., explosives) is worthy of mention. The industrial application of 3D printing to manufacture energetics is to print complex shapes for use as explosives, propellants, pyrotechnics, and warheads. However, these same capabilities could be used to print improvised explosive devices for use in assassinations or mass-casualty attacks. The authors of a 2022 article concluded that "generalizable methods for energetic material molding remain challenging."[53] Despite this assessment, by the end of the ten-year period of consideration, such capabilities are likely to be available as "additive manufacturing shows the potential to significantly reduce the time and cost expenses associated with prototyping, transportation, and application of functional [explosive] devices while reducing the lifecycle environmental impact."[54]

The economic impact of AM is challenging to predict. It will depend on how rapidly the technology continues to proliferate. The 24.3-percent annual global projected growth rate from 2022 to 2030 signals the market's potential; however, even a $100-billion market by 2030 is likely not transformative for the broader manufacturing market. Still, for DHS, the shift to AM, even if saturating only those six previously identified industries, could have important implications that the department would need to consider in terms of its responsibilities for border security, export controls, and customs enforcement.[55]

Anticounterfeiting measures exist, such as embedding tagging materials, micro–quick-response (QR) codes, or visible or fluorescent light features into metal or polymer printing materials and designs.[56] Although more research is necessary to make tagging more practical on an industrial scale, this technology is becoming important to companies that want to trace their products, preventing liability in the case of failure of a manufactured device, and detecting counterfeits.[57] One should expect that such measures will continue being developed for protecting IP and economic investments.

CONSEQUENCE

Consequences vary greatly depending on the industry in which the 3D printing technology is being employed. In some cases, it could result in annoyances when a product does not meet the stated technology specifications; in other cases, the stakes could be far higher and could even pose a threat to human lives.

AM is already being used in safety-critical products, such as turbine blades for airplanes, customized tools, and medical implants. The failure of any of these devices could cause injury or death, and they come from highly visible industries in which failures are not well tolerated. In fact, these industries have sought to ensure that 3D printed parts have failure modes that are understood and have been assessed for overall risk.

Despite the potential for high-consequence incidents involving 3D printed counterfeits during the ten-year time horizon of this study, we assessed that such incidents are likely to be more locally confined and unlikely to result in widespread and large-scale catastrophic events. The economic consequences could also be significant, causing loss of revenue for the legitimate manufacturers, loss of tax revenue, and losses as a result of accidents involving subpar counterfeited 3D printed materials. Counterfeit products already cause significant losses for many industries; we assessed that AM will exacerbate this problem because of its growing availability. However, we expect such losses to be confined as well, perhaps to no more than a handful of companies.

In making these assessments, we recognize that serious, even catastrophic outcomes can result from both localized and large-scale failures. For example, failure of a specific part can have catastrophic implications for people on a plane, but the need to investigate that part's failure across all planes to ensure safety can also have large-scale economic implications.

EMERGING TECHNOLOGY RISK ASSESSMENT

An overarching conclusion supported by our research and analysis is that AM offers new capabilities for developing and proliferating new technologies. It also provides a basis for setting the conditions for counterfeiting technologies. However, in this regard, AM is also affected by many of the same factors related to the protection of other emerging technologies, such as ensuring adequate cybersecurity to guard IP, ensuring key data protections, and retaining proprietary methods and processes. Table 2 provides our AM risk assessment.

In developing our technology assessment, we assessed a variety of **threat** actors across multiple use cases. In doing so, it was instructive to think about how such actors as foreign governments, nonstate actors (or terrorists), criminal organizations, and lone wolves could employ AM. To this end, we considered the potential **vulnerability** of counterfeiting untraceable and primitive firearms, improvised explosive devices, weapons of mass destruction, and other weapons that could be developed by employing AM technologies. Our assessment was that, despite advances in 3D printing, several of the less capable actors would likely be challenged to develop the weapons that would be the most sophisticated and most dangerous. For example, a lone wolf, a criminal organization, and even a nonstate actor would likely be challenged to gain access to material to produce a weapon of mass destruction.[58] We assessed that the same conclusion would apply to other technology areas. That is, 3D printing offers great capabilities, but often other supporting technologies would be needed to realize those capabilities.

In making our assessment, we have concluded that many issues are similar across the counterfeit categories that we discussed, but **vulnerability** and **consequence** can be vastly different. As a result, we have considered

TABLE 2

ADDITIVE MANUFACTURING RISK ASSESSMENT

Scenario	T_{AV} Average	Threat	Vulnerability	Consequence	Average
Short term (up to 3 years)	3.5	2	3	1	2.4
Medium term (3–5 years)	3.9	2.5	3.5	1.5	2.9
Long term (5–10 years)	4.3	3	4	2	3.3

NOTE: The emerging technology risk assessment scale is 0 to < 2 = low impact or not likely feasible, 2 to < 4 = moderate impact or possible, and 4 to 5 = high impact or likely feasible.

DHS components and headquarters elements should consider raising the visibility of the risks of AM.

the risks associated with the counterfeiting of a critical infrastructure technology that could fail and result in deaths and injuries. We also recognize conceptually the economic and IP rights impacts of counterfeiting. However, we made no attempt to quantify these impacts because the 2030 projection of approximately $100 million in annual AM production is dwarfed by the 2022 global manufacturing production total of $44.5 trillion.[59]

We assessed that, during the ten-year period under consideration, the T_{AV} will go from moderate or possible in the short term to high or likely feasible in the long-term assessment—this rating indicates a risk assessment of moderate and feasible.

We assessed that the number of **threat** actors with access to 3D printers and the knowledge to use them will continue to increase. Threat actors will also continue to have greater access to 3D printers that are more sophisticated and a wider variety of materials that will aid them in custom-designing specialized technologies and products, including counterfeit goods. We assessed that the **vulnerability** resulting from 3D printed counterfeit products and technologies will also continue to increase as more sophisticated 3D printers become available and the types and complexity of the materials that can be 3D printed grow. The **vulnerabilities** and the associated **consequences** of 3D printed counterfeits will have implications on product safety, the economy, IP issues, and the printing of illicit or banned products. Furthermore, we assessed that advances in AM will continue to be fueled by scientific discovery and technology development in AI, materials sciences, biology, chemistry, and nanotechnology, to name a few.

U.S. DEPARTMENT OF HOMELAND SECURITY EQUITIES

DHS has important responsibilities in securing the homeland and protecting and supporting the U.S. economy in such areas as border security, export controls, and customs enforcement that are contained in “more than 1,000 foundational documents, including federal statutes, EOs, presidential policy directives, homeland security presidential directives, DHS management directives, and DHS delegations.”[60] Although these responsibilities lie primarily with U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the U.S. Coast Guard, most DHS management headquarters and components have some responsibilities for or overlap with border security, export controls, and customs enforcement.[61]

Seizures of counterfeit goods at U.S. borders increased tenfold between 2000 and 2018, from 3,244 seizures per year to 33,810.[62] With the continued proliferation of AM and the difficulty that presents in identifying which goods have been counterfeited, this is an issue of high interest to DHS. In addition to the physical spread of goods, the digital spread of instructions that violate IP or ownership laws or are obtained through hacking involves other DHS entities, such as the Cybersecurity and Infrastructure Security Agency (CISA).

DHS components and headquarters elements should consider raising the visibility of the risks of AM—specifically, to mitigate vulnerabilities, develop protocols to more fully account for the changes wrought by 3D printing, and reduce negative consequences associated with the counterfeiting of 3D printed products. This could be done beginning with individual sectors that have been highlighted as industry leaders in AM: health care, aerospace, education, manufacturing, automotive, and robotics.[63]

The overlapping policy, legal, ethical, and regulatory issues inherent in AM demonstrate why such frameworks are complex to establish and should focus on both AM capabilities and their use cases. This overlap has implications for collaboration across the interagency; for example, in commercial aviation, the Federal Aviation Administration, the Transportation Security Administration, CISA, and aviation trade associations all have a stake in addressing these policy, legal, ethical, and regulatory issues.

CONCLUSION

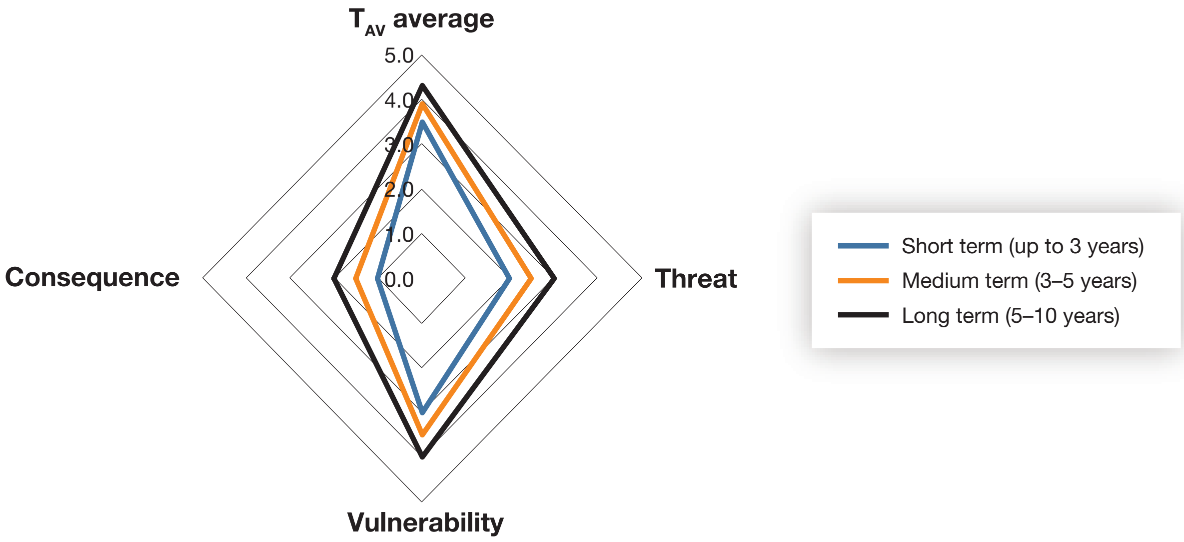
AM is not a new technology, but it is a rapidly growing field with increasing prospects for additional use cases and continued growth. Our analysis of AM, which focused on the risks associated with counterfeiting products, indicates that this technology is continuing to mature. This maturation results from the intersection of improved 3D printers and newly available materials. Although the number and type of use cases of AM will continue to grow, as evidenced by predictions of more than a 24-percent annual increase in revenue from 2022 to 2030, AM will likely remain focused largely in a handful of key areas.

We also assessed that counterfeits will have implications in a wide variety of areas, including product safety, the economy, IP issues, and the printing of illicit or banned products. Furthermore, we assessed that advances in AM will continue to be fueled by scientific discovery and technology development in converging fields, such as AI, materials sciences, biology, chemistry, and nanotechnology. These converging technologies have the potential to dramatically increase the annual growth projections for AM, which could result in a corresponding increase in associated risks, including for counterfeiting. Figure 2 provides our overall risk assessment (by period).

Overall, we assessed that the technology will continue to mature over the ten-year horizon of the analysis. The number of threat actors with access to these capabilities is likely to grow as the technology proliferates. In the vulnerability assessment, we determined that anticounterfeiting measures, such as tagging, that are in development will likely come to fruition by the end of the study period—however, this will not offset the increasing vulnerability resulting from the continued proliferation of the AM technology. Despite the potential for high-consequence incidents involving 3D printed counterfeits during the ten-year time horizon of the study, we assessed that these incidents are likely to be more locally confined and unlikely to result in widespread events, which places them in the moderate risk category. These assessments could change if done for a longer time horizon.

FIGURE 2

ADDITIVE MANUFACTURING RISK ASSESSMENT



NOTE: The emerging technology risk assessment scale is 0 to < 2 = low impact or not likely feasible, 2 to < 4 = moderate impact or possible, and 4 to 5 = high impact or likely feasible.

NOTES

[1] "3D Printing of Weapons: A Threat to Global, National, and Personal Security."

[2] "3D Printing of Weapons: A Threat to Global, National, and Personal Security."

[3] White, "3D Printing to Wipe Out 25% of World Trade by 2060."

[4] Mellor, Hao, and Zhang, "Additive Manufacturing," quoting ASTM International, "Standard Terminology for Additive Manufacturing Technologies."

[5] Additive Manufacturing Research Group, "About Additive Manufacturing."

[6] ASTM International, "Standard Terminology for Additive Manufacturing Technologies."

[7] Markforged, "Additive Manufacturing History."

[8] Axsom, "3D Printing."

[9] This framework is described in Chapter 6 and Appendix B of Gerstein, *The Story of Technology*.

[10] Welding Institute, "What Are the Advantages and Disadvantages of 3D Printing?"

[11] Formlabs, *Guide to Selective Laser Sintering (SLS) 3D Printing*.

[12] Formlabs, *Guide to Selective Laser Sintering (SLS) 3D Printing*.

[13] Emerging Technologies Subcommittee, "Final Report of the Emerging Technologies Subcommittee."

[14] Zaske, "Manufacturing on Mars with 3D Printing."

[15] Huning et al., "3D-Printed Nuclear Reactor Promises Faster, More Economical Path to Nuclear Energy"

[16] Lai, "First Thermoset 3D Printer Unveiled at Oak Ridge National Laboratory."

[17] Wattles, "Startup's 3D-Printed Rocket Delivers Stunning Night Launch but Fails to Reach Orbit."

[18] Hogan, "3D Printing with Polymers."

[19] Beesley, "NASA Looks to Build Habitats on Other Plants Using 3D Printing."

[20] Tzounis and Bangeas, "3D Printing and Nanotechnology."

[21] Linke, "Additive Manufacturing, Explained."

[22] Linke, "Additive Manufacturing, Explained."

[23] Lettori et al., "Additive Manufacturing Adoption in Product Design"; Business Wire, "Global 3D Printing Market Report 2022–2030."

[24] Schwaar, "2023 Additive Manufacturing Outlook."

[25] Schwaar, "2023 Additive Manufacturing Outlook."

[26] de Zeeuw, "Qualifying Aerospace Parts."

[27] Fortune Business Insights, *Aerospace 3D Printing Market Size*.

[28] de Zeeuw, "Qualifying Aerospace Parts."

[29] Jakk, "The Benefits of 3D Printing in Drone Making."

[30] Boeing, "'Seeing Red.'"

[31] Edwards, "Boeing Accelerates T-7 Development Using 3D Tools."

[32] Emerging Technologies Subcommittee, "Final Report of the Emerging Technologies Subcommittee."

[33] Emerging Technologies Subcommittee, "Final Report of the Emerging Technologies Subcommittee."

[34] Business Wire, "Global 3D Printing Market Report 2022–2030."

[35] Schneider, "3D-Printed Guns Are Getting More Capable and Accessible."

[36] Listek, "New US Federal Rule Treats 3D Printed Guns Like Any Other Firearm."

[37] Code of Federal Regulations, International Traffic in Arms Regulations, 22 C.F.R. Parts 120–130.

[38] Code of Federal Regulations, Export Administration Regulations, 15 C.F.R. Parts 730–774; Hanaphy, "U.S. Bureau of Industry and Security Imposes 'EAR' Restrictions on 3D Printed Guns."

[39] Porter, "What Is ITAR Compliance?"

[40] Bureau of Industry and Security, "BIS Imposes $2.77 Million Penalty on 3D Printing Company for Exports to China and Germany."

[41] Vogel, "Intellectual Property and Additive Manufacturing."

[42] Irving, "Four Ways 3D Printing May Threaten Security."

[43] Irving, "Four Ways 3D Printing May Threaten Security."

[44] Yeong and Chua, "A Quality Management Framework for Implementing Additive Manufacturing of Medical Devices."

[45] Zhang et al., "Three-Dimensional Printing of Energetic Materials."

[46] For this risk assessment, our determination of the threat focused on the capabilities and intentions of the actor; the vulnerabilities were weaknesses to be exploited; and the consequences were the outcomes of the event occurrence (Cox, "Some Limitations of 'Risk = Threat × Vulnerability × Consequence' for Risk Analysis of Terrorist Attacks").

[47] Tamim, "UK Develops 3D-Printed 'Suicide Drone' to Aid Ukraine Against Russia."

[48] Satam, "Russia's New UAV with 'Do-It-Yourself' Feature."

[49] Axsom, "3D Printing."

[50] Kilkenny, "3D Printed Rocket Launched Using Innovative NASA Alloy."

[51] Widmer and Rajan, "3D Opportunity for Intellectual Property Risk."

[52] Bitfab, "The Definitive Guide to Solving 3D Printing Problems."

[53] Zhang et al., "Three-Dimensional Printing of Energetic Materials," p. 98.

[54] Muravyev et al., "Progress in Additive Manufacturing of Energetic Materials," p. 962.

[55] As noted in Gerstein and Ligor, *Economic Security and the U.S. Department of Homeland Security*, "The department's primary sources of economic authority reside in more than 1,000 foundational documents, including federal statutes, EOs [executive orders], presidential policy directives, homeland security presidential directives, DHS management directives, and DHS delegations. [footnote omitted] And many of these authorities either directly or indirectly pertain to or affect economic U.S. security" (pp. 8–9). These include such areas as border screening, export controls, and customs enforcement. "The department's foundational documents—the Homeland Security Act (Pub. L. 107-296, 2002) (affecting approximately 900 statutory sections) and the department's directives (277) and delegations (23)—are sources to identify the universe of laws, regulations, EOs, presidential policy directives, and homeland security presidential directives covering DHS's entire jurisdiction" (Gerstein and Ligor, *Economic Security and the U.S. Department of Homeland Security*, p. 13).

[56] Wei et al., "Embedding Anti-Counterfeiting Features in Metallic Components via Multiple Material Additive Manufacturing."

[57] Sola et al., "How Can We Provide Additively Manufactured Parts with a Fingerprint?"

[58] Stehn et al., *3D Opportunity for Adversaries*.

[59] Jensen, "Global Manufacturing Production to Reach Value of $44.5 Trillion in 2022."

[60] Gerstein and Ligor, *Economic Security and the U.S. Department of Homeland Security*, p. 8.

[61] Gerstein and Ligor, *Economic Security and the U.S. Department of Homeland Security*.

[62] Office of Strategy, Policy and Plans, *Combating Trafficking in Counterfeit and Pirated Goods*

[63] Axsom, "3D Printing."

REFERENCES

"3D Printing of Weapons: A Threat to Global, National, and Personal Security," *Homeland Security News Wire*, May 14, 2018.

Additive Manufacturing Research Group, Loughborough University, "About Additive Manufacturing," webpage, undated. As of October 4, 2023: https://www.lboro.ac.uk/research/amrg/about/materials/

ASTM International, "Standard Terminology for Additive Manufacturing Technologies," F2792-12, last updated March 21, 2012.

Axsom, Tessa, "3D Printing: It's Time," Fictiv, July 10, 2023.

Beesley, Caron, "NASA Looks to Build Habitats on Other Planets Using 3D Printing," GovDesignHub, August 21, 2018.

Bitfab, "The Definitive Guide to Solving 3D Printing Problems," webpage, undated. As of October 4, 2023: https://bitfab.io/blog/3d-printing-problems

Boeing, "'Seeing Red,' T-7A Red Hawk 'Red Tail' Jet Makes Production Debut: Advanced U.S. Air Force Trainer Honors Tuskegee Airmen," April 28, 2022.

Bureau of Industry and Security, U.S. Department of Commerce, "BIS Imposes $2.77 Million Penalty on 3D Printing Company for Exports to China and Germany, Including Aerospace and Military Design Documents," press release, February 27, 2023.

Business Wire, "Global 3D Printing Market Report 2022–2030: Sector to Reach $105.4 Billion by 2030 at a 24.3% CAGR," *Research and Markets*, April 6, 2023.

Code of Federal Regulations, Title 15, Commerce and Foreign Trade; Subtitle B, Regulations Relating to Commerce and Foreign Trade; Chapter VII, Bureau of Industry and Security, Department of Commerce; Subchapter C, Export Administration Regulations.

Code of Federal Regulations, Title 22, Foreign Relations; Chapter I, Department of State; Subchapter M, International Traffic in Arms Regulations.

Cox, Louis Anthony, Jr., "Some Limitations of 'Risk = Threat × Vulnerability × Consequence' for Risk Analysis of Terrorist Attacks," *Risk Analysis*, Vol. 28, No. 6, December 2008.

de Zeeuw, Erik, "Qualifying Aerospace Parts: The True Roadblock Slowing AM's Rise," Materialise, undated.

Edwards, Jane, "Boeing Accelerates T-7 Development Using 3D Tools, Model-Based Engineering; Paul Niewald Quoted," *ExecutiveBiz*, December 20, 2021.

Emerging Technologies Subcommittee, Homeland Security Advisory Council, U.S. Department of Homeland Security, "Final Report of the Emerging Technologies Subcommittee: 3D-Printing," February 24, 2020.

Formlabs, *Guide to Selective Laser Sintering (SLS) 3D Printing*, white paper, January 2021.

Fortune Business Insights, *Aerospace 3D Printing Market Size, Share, Growth and COVID-19 Impact Analysis, by Vertical (Printers, Materials), by Industry (UAVs, Aviation, and Space), by Application (Engine Components, Space Components, and Structural Components), by Printer Technology (DMLS, FDM, CLIP, SLA, SLS, and Others), and Regional Forecast, 2022–2029*, FBI101613, November 2022.

Gerstein, Daniel M., *The Story of Technology: How We Got Here and What the Future Holds*, Prometheus Books, 2019.

Gerstein, Daniel M., and Douglas C. Ligor, *Economic Security and the U.S. Department of Homeland Security: Addressing a Changed World and Evolved Threat Landscape*, RAND Corporation, PE-A2210-1, April 2023. As of October 4, 2023: https://www.rand.org/pubs/perspectives/PEA2210-1.html

Hanaphy, Paul, "U.S. Bureau of Industry and Security Imposes 'EAR' Restrictions on 3D Printed Guns," *3D Printed Industry*, July 22, 2021.

Hogan, Madeline, "3D Printing with Polymers: The Complete Guide for 2023," Nexa3D, undated.

Huning, Alex J., Kory D. Linton, Andrew T. Nelson, Vincent C. Paquit, Nicholas J. Prins, T. S. Byun, and Will M. Kirkland, "3D-Printed Nuclear Reactor Promises Faster, More Economical Path to Nuclear Energy," Oak Ridge National Laboratory, May 11, 2020.

Irving, Doug, "Four Ways 3D Printing May Threaten Security," *RAND Blog*, May 8, 2018. As of October 5, 2023: https://www.rand.org/blog/articles/2018/05/four-ways-3d-printing-may-threaten-security.html

Jakk, "The Benefits of 3D Printing in Drone Making," *Additive-X*, blog post, undated. As of October 4, 2023: https://additive-x.com/blog/the-benefits-of-3d-printing-in-drone-making/

Jensen, Sara, "Global Manufacturing Production to Reach Value of $44.5 Trillion in 2022," *Power and Motion*, May 31, 2022. As of October 5, 2023: https://www.powermotiontech.com/news/article/21242721/global-manufacturing-production-to-reach-value-of-445-trillion-in-2022

Kilkenny, Nancy Smith, "3D Printed Rocket Launched Using Innovative NASA Alloy," National Aeronautics and Space Administration, May 2, 2023.

Lai, Eric, "First Thermoset 3D Printer Unveiled at Oak Ridge National Laboratory," *3D Printing Industry*, April 13, 2018.

Lettori, Jacopo, Roberto Raffaeli, Margherita Peruzzini, Juliana Schmidt, and Marcello Pellicciari, "Additive Manufacturing Adoption in Product Design: An Overview from Literature and Industry," *Procedia Manufacturing*, Vol. 51, 2020.

Linke, Rebecca, "Additive Manufacturing, Explained," Massachusetts Institute of Technology Sloan School of Management, December 7, 2017.

Listek, Vanesa, "New US Federal Rule Treats 3D Printed Guns Like Any Other Firearm," 3DPrint.com, August 30, 2022.

Markforged, "Additive Manufacturing History: From the 1980's to Now," webpage, undated. As of October 4, 2023: https://markforged.com/resources/blog/additive-manufacturing-history

Mellor, Stephen, Liang Hao, and David Zhang, "Additive Manufacturing: A Framework for Implementation," *International Journal of Production Economics*, Vol. 149, March 2014.

Muravyev, Nikita V., Konstantin A. Monogarov, Uwe Schaller, Igor V. Fomenkov, and Alla N. Pivkina, "Progress in Additive Manufacturing of Energetic Materials: Creating the Reactive Microstructures with High Potential of Applications," *Propellants, Explosives, Pyrotechnics*, Vol. 44, No. 8, August 2019.

Office of Strategy, Policy and Plans, U.S. Department of Homeland Security, *Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States*, January 24, 2020.

Porter, Alexis, "What Is ITAR Compliance? Safeguard Your Data," *BigID*, blog post, February 2, 2023. As of October 4, 2023: https://bigid.com/blog/what-is-itar-compliance/

Public Law 107-296, Homeland Security Act of 2002, November 25, 2002.

Satam, "Russia's New UAV with 'Do-It-Yourself' Feature, 3D Printed and Strapped with RPG-7 Aims to Hunt Ukraine's Tanks," *EurAsian Times*, May 14, 2023.

Schneider, Ari, "3D-Printed Guns Are Getting More Capable and Accessible," *Future Tense*, February 16, 2021.

Schwaar, Carolyn, "2023 Additive Manufacturing Outlook: Industry Leaders on the Year Ahead," *All3DP*, December 20, 2022.

Sola, Antonella, Yilin Sai, Adrian Trinchi, Clement Chu, Shirley Shen, and Shiping Chen, “How Can We Provide Additively Manufactured Parts with a Fingerprint? A Review of Tagging Strategies in Additive Manufacturing,” *Materials*, Vol. 15, No. 1, 2022.

Stehn, Mike, Ian Wing, Tina Carlile, Joe Dichairo, and Joe Mariani, *3D Opportunity for Adversaries: Additive Manufacturing Considerations for National Security*, Deloitte University Press, 2017.

Tamim, Baba, “UK Develops 3D-Printed ‘Suicide Drone’ to Aid Ukraine Against Russia,” *Interesting Engineering*, February 18, 2023.

Tzounis, Lazaros, and Petros Bangeas, “3D Printing and Nanotechnology,” in Vasileios N. Papadopoulos, Vassilios Tsioukas, and Jasjit S. Suri, eds., *3D Printing: Applications in Medicine and Surgery*, Vol. 2, 2022.

U.S. Code, Title 6, Domestic Security; Chapter 1, Homeland Security Organization; Subchapter III, Science and Technology in Support of Homeland Security; Section 185, Federally Funded Research and Development Centers.

Vogel, Bryan J., “Intellectual Property and Additive Manufacturing/3D Printing: Strategies and Challenges of Applying Traditional IP Laws to a Transformative Technology,” *Minnesota Journal of Law, Science and Technology*, Vol. 17, No. 2, June 2016.

Wattles, Jackie, “Startup’s 3D-Printed Rocket Delivers Stunning Night Launch but Fails to Reach Orbit,” CNN Business, March 23, 2023.

Wei, Chao, Zhe Sun, Yihe Huang, and Lin Li, “Embedding Anti-Counterfeiting Features in Metallic Components via Multiple Material Additive Manufacturing,” *Additive Manufacturing*, Vol. 24, December 2018.

Welding Institute, “What Are the Advantages and Disadvantages of 3D Printing?” webpage, undated. As of October 5, 2023: https://www.twi-global.com/technical-knowledge/faqs/what-is-3d-printing/pros-and-cons

White, Edward, “3D Printing to Wipe Out 25% of World Trade by 2060: Report,” *Financial Times*, September 29, 2017.

Widmer, Matt, and Vikram Rajan, “3D Opportunity for Intellectual Property Risk: Additive Manufacturing Stakes Its Claim,” Deloitte University Press, 2016.

Yeong, Wai Yee, and Chee Kai Chua, “A Quality Management Framework for Implementing Additive Manufacturing of Medical Devices,” *Virtual and Physical Prototyping*, Vol. 8, No. 3, 2013.

Zaske, Sara, “Manufacturing on Mars with 3D Printing,” *Tech Briefs*, December 1, 2022.

Zhang, Ji-chi, Kuai He, Da-wei Zhang, Ji-dong Dong, Bing Li, Yi-jie Liu, Guo-lin Gao, and Zai-xing Jiang, “Three-Dimensional Printing of Energetic Materials: A Review,” *Energetic Materials Frontiers*, Vol. 3, No. 2, June 2022.

ABBREVIATIONS

3D	three dimensional
4D	four dimensional
AI	artificial intelligence
AM	additive manufacturing
CISA	Cybersecurity and Infrastructure Security Agency
DHS	U.S. Department of Homeland Security
EO	executive order
IP	intellectual property
R_S	risks and scenarios
T_{AV}	technology availability
TRL	technology readiness level

About the Authors

Daniel M. Gerstein works at the RAND Corporation. From 2011 to 2014, he served as the Acting Under Secretary and Deputy Under Secretary of the DHS Science and Technology Directorate. He has a doctorate in biodefense.

Erin Leidy is a technical analyst at RAND. Some of her areas of interest are in emerging technology, science policy, cybersecurity, and technology implementation. She has an M.S. in technology policy.

ABOUT THIS REPORT

This report is part of a series of analyses on the effects of emerging technologies on U.S. Department of Homeland Security (DHS) missions and capabilities. As part of this series, the Homeland Security Operational Analysis Center (HSOAC) was charged with developing a technology and risk assessment methodology for evaluating emerging technologies and understanding their implications within a homeland security context. This report is intended to inform DHS's Science and Technology Directorate and Office of Policy on the implications of additive manufacturing.

This research was sponsored by the DHS Science and Technology Directorate and conducted in the Management, Technology, and Capabilities Program of the RAND Homeland Security Research Division, which operates HSOAC.

HSOAC
HOMELAND SECURITY
OPERATIONAL ANALYSIS CENTER

An FFRDC operated by the
RAND Corporation under
contract with DHS

The Homeland Security Act of 2002 authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. The RAND Corporation operates the Homeland Security Operational Analysis Center (HSOAC) as an FFRDC for DHS under contract HSHQDC-16-D-00007.

The HSOAC FFRDC provides the government with independent and objective analyses and advice in core areas important to the Department in support of policy development, decisionmaking, alternative approaches, and new ideas on issues of significance. The HSOAC FFRDC also works with and supports other federal, state, local, tribal, and public- and private-sector organizations that make up the homeland security enterprise. The HSOAC FFRDC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks.

The information presented in this publication does not necessarily reflect official DHS opinion or policy.

For more information on this publication, visit www.rand.org/t/RRA2984-1.

This research was published in 2024.

RR-A2984-1