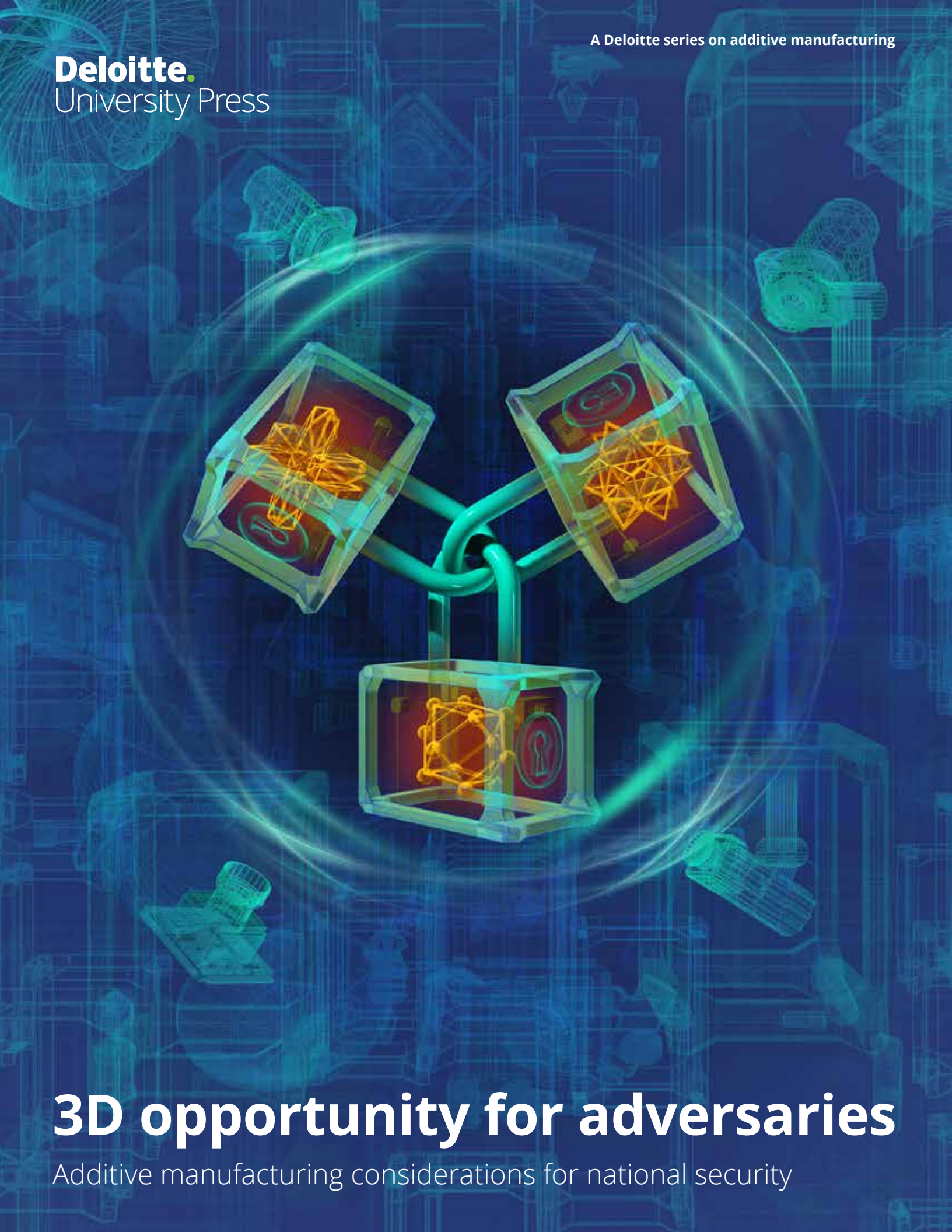
A Deloitte series on additive manufacturing

Deloitte.
University Press

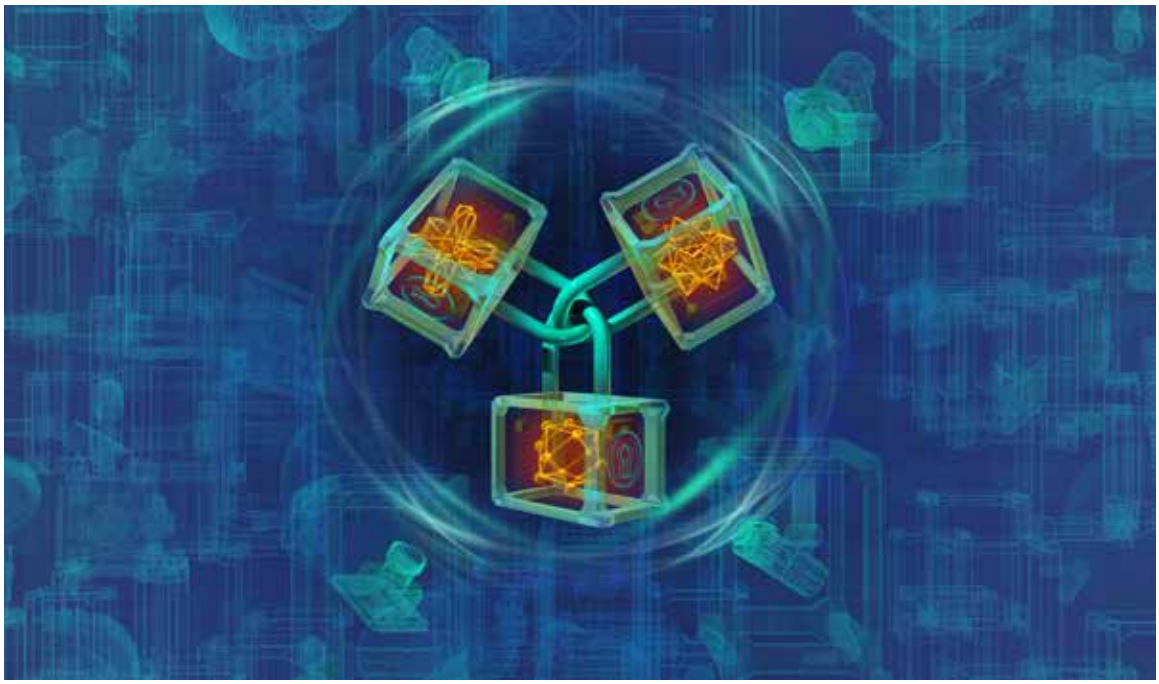


3D opportunity for adversaries

Additive manufacturing considerations for national security

COVER IMAGE BY: J.F. PODEVIN

CONTENTS



Introduction

In 2013, Cody Wilson, a self-described crypto-anarchist and gun-rights activist, posted blueprints for the Liberator, a functioning one-shot plastic pistol that could be reproduced with a 3D printer, via additive manufacturing. Local law enforcement had no issues with it—a resident of Texas, Wilson had been issued a federal license to manufacture and deal in firearms.[1]

It was the US Department of State, through its Directorate of Defense Trade Controls, that requested the files be taken down until a determination could be made whether the information was controlled "technical data."[2] It claimed that the files were potentially subject to a set of regulations known as the US International Traffic in Arms Regulations (ITAR). The State Department's position was that publishing "technical data," a term defined under US law, which includes information used for the development, production, or use of an export-controlled item, was tantamount to the export of technical data and that Wilson did so without authorization.[3]

Wilson eventually complied—but not before the files for the gun had been downloaded over 100,000 times.[4] In 2015, Defense Distributed, a nonprofit founded and run by Wilson, and the gun rights group Second Amendment Foundation filed a lawsuit against the State Department, claiming a violation of Wilson's first-amendment right to free speech.[5]

THIS case highlights one of the trickier aspects of additive manufacturing (AM), also known as 3D printing: The capabilities it enables can be applied beyond the bounds of legitimate businesses, and exploited by those seeking to do harm.

AM does not pose a threat in and of itself. Quite the opposite; AM can provide great benefits for society. At the same time, however, these benefits can also be used to malign ends. The same characteristics that make AM valuable to manufacturers—speed to delivery, on-demand production at or close to the point of use, more effective inventory management, design innovation, and lower barriers to entry into new geographies—may also attract those with malicious intent. AM makes these ends more attainable by democratizing access to technology. This can simultaneously create a new challenge for law enforcement, as the wider access to technology enabled by AM can make controlling the creation or possession of dangerous devices much more difficult.

Put simply, AM can make it easier to engage in certain types of threatening behavior that could undermine aspects of national security. By examining the impacts AM has on business (see the sidebar "The additive manufacturing framework"), this article strives to identify some of the potential threats and threat actors, examine some of the ways in which AM can potentially be put to malicious uses, and present a lens through which law enforcement, national security, and intelligence organizations from every nation can consider avenues to protect citizens.

THE ADDITIVE MANUFACTURING FRAMEWORK

AM's roots go back nearly three decades. Its importance is derived from its ability to break existing performance trade-offs in two fundamental ways. First, AM can reduce the capital required to achieve economies of scale. Second, it increases flexibility and reduces the capital required to achieve scope.[6]

Capital versus scale: Considerations of minimum efficient scale can shape supply chains. AM has the potential to reduce the capital required to reach minimum efficient scale for production, thus lowering the manufacturing barriers to entry for a given location.

Capital versus scope: Economies of scope influence how and what products can be made. The flexibility of AM facilitates an increase in the variety of products a unit of capital can produce, which can reduce the costs associated with production changeovers and customization and, thus, the overall amount of required capital.

Changing the capital versus scale relationship has the potential to impact how supply chains are configured, and changing the capital versus scope relationship has the potential to impact product designs. These impacts present companies with choices on how to deploy AM across their businesses.

Companies pursuing AM capabilities choose between divergent paths (figure 1):

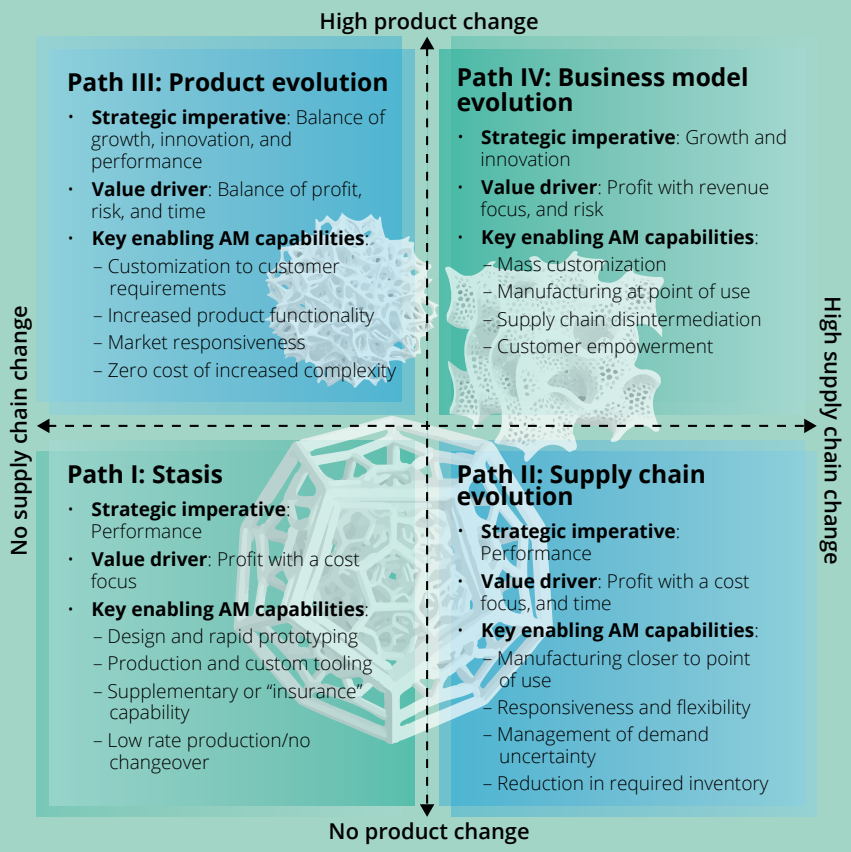
Path I: Companies do not seek radical alterations in either supply chains or products, but they may explore AM technologies to improve value delivery for current products within existing supply chains.

Path II: Companies take advantage of scale economics offered by AM as a potential enabler of supply chain transformation for the products they offer.

Path III: Companies take advantage of the scope economics offered by AM technologies to achieve new levels of performance or innovation in the products they offer.

Path IV: Companies alter both supply chains and products in pursuit of new business models.

Figure 1. Framework for understanding AM paths and value



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

Characterizing the threat

Different actors, same intent

In the national security context, a threat is characterized by a combination of intent and capability.[7] Before we explore the various ways in which AM can lower the barriers to entry for malicious actors, it is important to first identify who those various actors could be, and highlight some of the common threats by which they may typically act—threats that can be strengthened to some extent by the use of AM.

We will consider a representative cross section of potential actors. It is important to note, however, that in today's world, the points of demarcation between these actors are often blurry, and this list is not intended to be exhaustive:

- **Lone wolf:** It refers to an individual actor, operating independently to achieve his or her own goals. AM can increase the availability of technology, knowledge, and equipment, lowering the "barriers to entry" for such individuals while potentially increasing the impact of their actions.[8]
- **Organized crime:** A group of individuals can operate on a local, national, or transnational scale, performing illegal activities primarily motivated by economic (and sometimes political) factors. The highly organized, systematized approach to criminal activity used by these groups can undermine the rule of law and threaten national security itself, as evidenced by the activities of Latin American drug cartels.[9] While their levels of sophistication, internationalization, and politicization may vary, their illegal activities can be enhanced, and detection potentially evaded, through the use of AM.
- **Non-state (terrorist) actors:** A well-organized network of determined actors can use violence to achieve geopolitical goals. Non-state networks are differentiated from the other categories in that their organizing principle is overtly political, and their objective in acquiring weaponry is to commit acts of terror and cause fear.[10] AM can help terrorist groups not only acquire new weapons or capabilities, but also allow them to do so more rapidly and stealthily than before, across a wider range of locations.
- **National strategy of a foreign government:** It refers to the coordinated actions of a foreign government taken to advance its geopolitical agenda. In contrast to the other actor categories, nation–states possess significant industrial and financial resources, which can permit sanctioned activity to happen within their borders, despite international efforts to delay or deter it. AM is but one tool at their disposal.[11]

AM significantly reduces the barriers to entry in many technological fields, democratizing the capabilities to do harm and potentially introducing new, asymmetric threats.

While these groups may differ, the intent remains a constant thread that all share in common: Each group has the intent do to harm, regardless of whether AM is involved. Therefore, the real impact of AM is on the capability side of the threat definition. AM significantly reduces the barriers to entry in many technological fields, democratizing the capabilities to do harm and potentially introducing new, asymmetric threats. The automated nature of AM and the manufacturing flexibility it affords means that the physical, logistical, and human capital requirements to run a small/agile manufacturing operation are less prohibitive.

For purposes of discussion, we will consider five use cases that could be either created directly or improved by AM.[12]

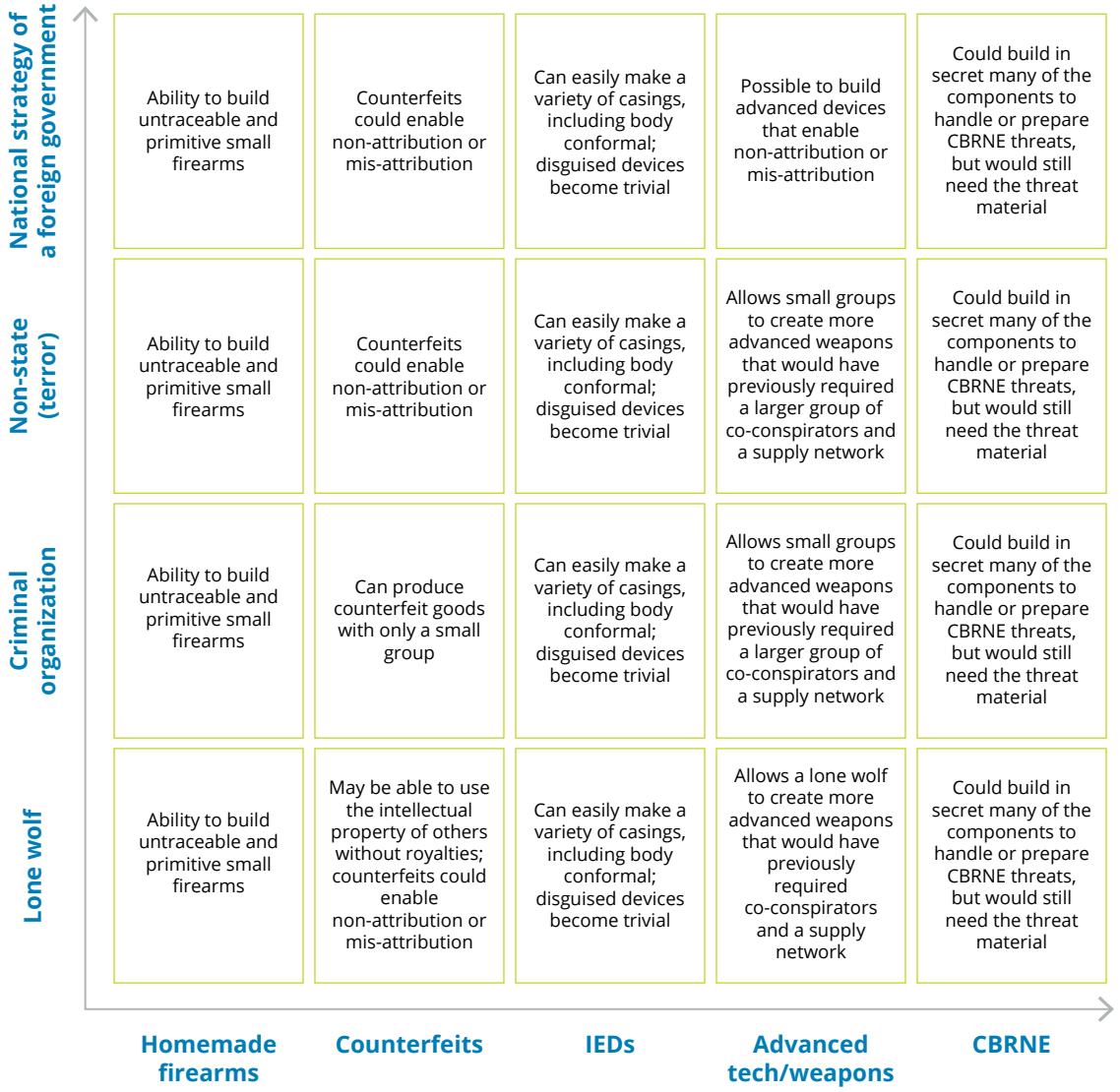
- **Homemade firearms:** Improvised plastic firearms made on hobby-grade additive manufacturing machines with plans downloaded from the Internet[13]
- **Counterfeits:** Goods or components designed and produced to mimic a trusted product from a trusted supplier;[14] products can range from counterfeit consumer goods, to credit card scanners, and even include false parts for military hardware[15]
- **Improvised explosive devices:** Nontraditional explosive devices[16]
- **Advanced technology/weapons:** A collection of advanced, usually export-controlled, technologies, including jet engine technology, missile technology, and advanced explosive systems such as explosively formed penetrators (EFPs)[17]
- **CBRNE threats:** Chemical, biological, radiological, nuclear, and explosive (CBRNE) threats, as well as the means to produce or accelerate production/weaponization of such threats[18]

Considering these two dimensions of actor and AM-produced categories as a matrix, and arranging them roughly in order of sophistication, we depict the threat/actor space in figure 2.

Of course, the true threat space is limited only by human imagination. This presents a challenge for those whose responsibility it is to protect the population. How can they anticipate a criminal's imagination and therefore take action ahead of time to protect against a threat?

In the next section, we explore how the AM framework—a set of paths that guide the ways in which businesses and government agencies can extract value from AM—can also be exploited by those seeking to do harm. As we do so, we will explore the ways in which AM can help enable some of the specific threats identified in figure 2.

Figure 2. Sample threat matrix



Source: Deloitte analysis.

Opportunities and threats

Two sides of the coin

THE AM framework identifies opportunities that the technology creates for companies and government entities in a commercial or industrial setting. But its benefits can be a double-edged sword, streamlining processes for criminal actors and posing a threat to national security. The threat actors discussed above are admittedly not companies, but they can be similarly well-organized, and seek to use many of the same tools and strategies as legitimate organizations to achieve their desired ends—only with, to be sure, a *very* different set of objectives. As they pursue their goals, however, they can still exploit the benefits of AM to break the trade-offs between scale and scope in much the same way companies do: to test and develop new devices more quickly, sidestep the supply chain, produce wholly new objects, or manufacture a wider variety of them more easily.

In fact, precisely because they are unfettered by many of the rules of society, the threat actors can often be at the forefront of adopting new technology, meaning that those tasked to protect society may already lag behind their adversaries. For example, at the turn of the last century, criminals were quick to see the utility of automobiles, using them to escape from heists while police still walked or rode on horseback.[19] The problem was not that the police lacked imagination, but that they did not seem to understand ahead of time how the new technology could benefit criminals and therefore did not take appropriate action to prevent that use.

Thus, if we are to protect against malicious actors, it is crucial to understand how AM allows these bad actors to do new bad things, faster. Below, we explore some of the opportunities AM presents for new threats and the paths by which these threats can emerge.

Path I: Stasis

Businesses have already shown several ways to harness AM with minimal changes to their product or supply chain.[20] Even at this most accessible stage of AM usage, would-be threat agents can leverage the technology to enable economies of scope. Machines are inherently dual or even multiuse, meaning that an adversary could produce legitimate goods during business hours, and quickly convert to weapons or other contraband afterward. This has long been possible with traditional manufacturing, but the advent of AM dramatically lowers barriers to engaging in illegal behaviors by decreasing the time and cost associated with the changeover, complicating the detection and interdiction of such activity. Malicious actors can also leverage rapid prototyping to more easily create and test new ideas while wasting fewer resources.

A DEEPER LOOK AT POTENTIAL PATH I THREATS: ENABLING CBRNE

It can be difficult to imagine a scenario where a nuclear device is 3D printed from scratch—or a chemical, biological, radiological, or explosive weapon, for that matter. However, AM can still produce small parts on demand. Indeed, a February 2017 report from the Stockholm International Peace Research Institute (SIPRI) concluded that, at the current state of technological development, AM cannot be used in all parts of weapon development, but can be used to print miscellaneous noncritical components.[21]

A DEEPER LOOK AT POTENTIAL PATH I THREATS: ENABLING CBRNE CONT.

These components could be used in a number of applications, especially around the handling of weapons-grade nuclear material, including uranium enrichment, or tools for synthesizing chemical or biological compounds.[22] In this way, AM can ease the development of a covert or overt CBRNE weapons program by accelerating development, easing the process of handling and transporting dangerous materials, or enabling a low signature presence. Adversaries of all types can use AM to locally produce the mechanical components of laboratory equipment and specialized apparatus they need for developing or weaponizing materials. In this case, AM shortens breakout time and reduces traditional indicators and warnings.

Path II: Supply chain evolution

The impact of AM on the supply chain can have even larger implications for national security. Using AM, militaries can potentially disintermediate their supply chains and produce warfighting equipment locally, at the point of use.[23] This means that large, observable build-ups of materiel prior to invasions or other military action can be reduced. For the defense and government agencies responsible for monitoring such build-ups, AM potentially makes even large campaigns less predictable and therefore less prone to detection.

In much the same way that the US military seeks to deploy AM for maintenance and sustainment, smaller adversaries could achieve the same goals, reducing supply chain vulnerability and improving sustainment capabilities in a prolonged conflict. Further, large-scale adoption of AM could drastically reduce or eliminate reliance on identifiably military imports. As long as commercial imports—such as 3D printers—are allowed, the inherent dual-use nature of AM could still allow for production of military goods, effectively nullifying the effect of traditional weapons sanctions and export controls.

Use of AM along path II can also enable criminal organizations to sidestep typical smuggling approaches. This can have profound implications on detection of criminal activity, as US agencies can often track the movement of goods, such as illicit arms, to understand when and where threats may emerge.[24] If organizations can print parts, tools, or weapons on-site, they can amass needed supplies while making it far more difficult for agencies to track them and deduce their intent.

A DEEPER LOOK AT POTENTIAL PATH II THREATS: HOMEMADE FIREARMS

With today's technology, it is possible to manufacture a rudimentary firearm from plans on the Internet using a 3D printer, and supply it with standard ammunition.[25] Under current US federal law, however, no prohibition exists regarding the production of firearms for personal use. As of the writing of this paper, only a handful of states have sought to enact legislation to outlaw the use of AM to print guns.[26] Even in those cases that do reach a court, prosecutors may find themselves stymied by the law, which has not yet caught up to the technology, or the application of seemingly unrelated regulations as a defense, as in the story described at the outset of this article.

The total number of functioning guns and ammunition printed is impossible to calculate, but the ability to produce these types of weapons will likely only improve as printing technologies and material variety and quality continue to advance; in one case, a company claimed to have additively manufactured a gun that could shoot 200 rounds with minimal wear and tear.[27] As technology continues to improve and proliferate, it may become possible for more advanced, reliable firearms to be produced with AM technology. Further, AM can enable the production of firearms using materials that may be less easy to detect in a security screening.

A DEEPER LOOK AT POTENTIAL PATH II THREATS: HOMEMADE FIREARMS CONT.

While homemade firearms may pose less of a challenge in the United States, where it is relatively easy to access a factory-made gun either through legal means or the grey/black market, this is not necessarily true in other parts of the world where access to firearms is more constrained.

At the same time, even as regulations exist to control the sale and distribution of traditionally manufactured firearms, the ability to seek the technical "know-how" to print, procure the necessary AM materials, and purchase off-the-shelf printers to complete the printing remains relatively uncontrolled. This highlights the challenge facing law enforcement and national security experts: AM machines are commercially available, making it possible for anyone to access the technology. Questions about regulating the sale and use of AM printers and digital design files have arisen, but this remains a challenge.[28]

Path III: Product evolution

AM can also allow for the creation of entirely new products that can outperform their traditional counterparts. For example, scientists at Lawrence Livermore National Laboratory have discovered that AM is actually more suitable than traditional manufacturing for the creation of certain types of parts.[29] For example, plastic foams play a key role in the construction of thermonuclear weapons.[30] Foams created by traditional processes leave random spaces throughout a material. AM, on the other hand, is able to create regular spacing, resulting in a material that is more resilient and more durable than traditional foams and can even be tuned to specific applications.

AM's ability to effectively lower barriers to product innovation can have impacts on national security. It can make weapons and tools that previously were too difficult to procure or manufacture by other means more widely available to a variety of actors. For example, a terrorist organization might seek to create untraceable 3D-printed firearms or plastic bomb components specifically designed to evade airport security. These all could have been made previously, but would have been prohibitively difficult to design and produce using traditional manufacturing techniques. However, the design flexibility at low cost enabled by AM makes a variety of new designs possible for weapons, potentially invalidating proven security screening and countermeasures.

AM's ability to effectively lower barriers to product innovation can have impacts on national security.

For larger, more established actors, AM can also serve as both a catalyst and accelerator. Far from being the realm of science fiction, AM is already used within advanced weapons programs. For example, the US National Nuclear Safety Administration has printed more than 25,000 nonnuclear parts, creating products that weigh less and perform better than traditional counterparts.[31] While it is extremely unlikely that an adversary will directly 3D print a weapon of mass destruction, AM may be used in concert with other technologies, such as computer numerical control (CNC) machines, to produce small components or customized parts to be used within a larger weapon such as neutron reflectors or critical valves in production processes.[32] Often these intricate parts require long, iterative periods of design, testing, and calibration to ensure that they work correctly within the finished device. This extensive testing can be detected and traced, providing intelligence agencies and decision makers

A DEEPER LOOK AT POTENTIAL PATH III THREATS: THE DISGUISED THREAT

Terror groups have shown continued interest in and have been successful in smuggling explosive devices into controlled areas by disguising them as everyday objects.[34] This is not a new phenomenon, but the relative simplicity and ease with which threats can be disguised using AM may warrant special attention—and can expand beyond smuggling disguised explosives to other, more innovative approaches. For example, a group of criminals used a 3D printer to produce replica card slots (or "skimmers") for ATMs, which could be fitted over ATM machines. Using these disguised devices, the criminals were able to copy bank customers' information and use it to steal several hundred thousand dollars.[35]

with a relatively clear picture of the status of any illicit weapons program.[33] However, because an AM part can exist digitally long before it is ever made physical, initial digital testing can be potentially accomplished more covertly, making certain types of detection more difficult.

Path IV: Business model evolution

Business model evolution combines paths II and III, changing both product and supply chain, to create entirely new ways of doing business, whether your business is consumer goods or crime and mayhem. While the exact specifics of these new types of threat may not yet be known, the most significant "benefits" to malicious actors come when AM is combined with other, existing technologies to allow them to create entirely new criminal or military strategies. For example, in recent years, terrorist organizations have shown considerable prowess in using the Internet and social media to recruit operatives in target countries, making what was once a laborious and slow process perhaps faster and lowering geographical barriers.[36] An extension of this is to leverage the same platforms for the distribution of both attack commands and weapon designs to be used in entirely new forms of attack. Terrorist organizations can transmit instructions for an attack together with the files for creating weapons over the Internet. In this way, potential terrorists could participate independently in a simultaneous attack without any central direct planning or guidance.[37] The result could be not just a new weapon, but an entirely new form of attack: a distributed, simultaneous strike across the globe. While each attacker may cause only limited destruction, the combined effect could be much larger. Without any centralized planning to detect, such a novel form of attack could be very difficult to prevent.

A DEEPER LOOK AT POTENTIAL PATH IV THREATS: THE UNDETERMINED FUTURE

Just as it was nearly impossible to predict the success of ride-sharing or similar new business models, so too is it difficult to predict exactly what new strategies threat actors may adopt in the future. The ability of a threat actor with the intent to weaponize capabilities is limited only by their imagination. However, by using tools such as the four paths of AM, we can understand how those capabilities are likely to evolve and therefore stand ready for whatever new threat may emerge.

Protecting the population

A journey, not a destination

THE variety of potential threats—and the ways in which AM can be used—means that no single approach can protect against them all. Rather, the response to threatening uses of AM can involve everything from export regulations to surveillance of criminals to modifications to intelligence assessments, to considering ways to regulate digital files or track sales of machines. The effectiveness of these efforts may ultimately lie in their coordination. For example, law enforcement agents seeking to prevent the use of printed firearms may need help from intelligence agencies tracking the flow of design files on the dark web. Similarly, intelligence operatives seeking to understand the status of prohibited nuclear weapons programs may need support from diplomatic or economic experts on technology transfer, or even the AM industry itself. Regardless, the wide range of efforts required to counter the various threatening uses of AM means that numerous governmental and international organizations should be involved in that coordination.

The variety of potential threats—and the ways in which AM can be used—means that no single approach can protect against them all.

With this in mind, the following steps should be considered to protect against the negative uses of AM:

1. **Creating an international community of action:** Establishing mechanisms for government, industry, and international organizations to cooperate rapidly across traditional boundaries
2. **Working toward a common industry and international policy:** Beginning to work toward a single, clearly articulated policy that incorporates industry and international actors and governments

1. Creating an international community of action

Some progress has already been made in assembling a community of stakeholders interested in the possible threatening uses of AM. Several working groups within government are addressing the challenges posed by an adversary's use of additive manufacturing, including the US Department of Commerce Emerging Technology and Research Advisory Committee, which regularly holds meetings with industry and academia on emerging technologies. These meetings focus on examining the possibilities of new technologies and exploring what the appropriate controls for those technologies may be.[38]

However, while such organizations represent progress, there may be opportunity for even greater coordination across the different functions of government. The diversity of threats and actors means that full representation from governments—the United States and its allies, industry,

and international organizations—should be used to craft a comprehensive strategy. A single overlooked threat can create the exact national security incident that authorities are seeking to avoid.

2. Working toward a common industry and international policy

The creation of a community of action around AM is not the end, but rather the beginning of the cooperation necessary to adapt and react to such a rapidly changing technology. To guide this coordination and make it more meaningful than just a periodic conference, a common policy applicable to both industry and international actors is needed. While creating a common policy for AM acceptable to such a diverse community of stakeholders can seem daunting, lessons can be drawn from similar threats. In this regard, the situation regarding threats from AM is not dissimilar to that of improvised explosive devices (IEDs). In the effort to counter IEDs, the US government created an agile, coordinated community with roles and responsibilities articulated in Presidential Policy Directive 17 (PPD-17).[39] As with PPD-17, the first steps to creating the agility and coordination necessary to mitigate the threats from AM may be the creation of a coordinated national strategy. Such a strategy can assemble the appropriate stakeholders, help to define the issues, and begin to scope collaboration. While the specifics of that coordinated policy would necessarily evolve with circumstances, the pace of technological change will likely require some adjustments from all stakeholders.

MORE RAPID ANALYSIS

The potential for valid, commercial AM machinery to be put to use for undesirable purposes can increase the speed with which bad actors can produce weapons. This speed means that typical analytical tools and decision-making forums/methods should be adjusted. Faster intelligence analysis is needed to match the consolidated development timelines enabled by AM. Adjusting the time thresholds and values in analytical models can help to accommodate speed, make sense of new types of data coming in for analysis, and produce accurate assessments of the activity of terrorists and nation–states alike. National security decision-making forums can anticipate the need to address the negative use of AM. Novel analytical approaches evaluating the intent, opportunity, and impact of AM can help provide a more robust rapid analysis of this new threat. For example, one government agency is now leveraging "advanced computing and analytical solutions . . . to effectively combine and analyze multiple, large disparate data sets to increase enforcement effectiveness" against cross-border smuggling including counter-proliferation casework.[40] Similar approaches to AM could be widely useful across stakeholders.

NEW INDICATORS OF ACTIVITY

In order to tease valid conclusions from unclear data, the Intelligence Community has long used a list of key metrics—Indications and Warnings (I&W)—to drive intelligence collection and help predict a particular threat.[41] As AM disintermediates the supply

> The ability of AM to redefine the production processes from which many traditional intelligence indicators are derived can force governments to re-examine how they observe a threat, develop collection plans, and analyze information to support decision making.

chain, it can also change or challenge traditional intelligence I&W. Adversaries could potentially increase readiness, deploy troops, or create illegal weapons without advance warning.

The ability of AM to redefine the production processes from which many traditional intelligence indicators are derived can force governments to re-examine how they observe a threat, develop collection plans, and analyze information to support decision making. Given the rapid flow of digital information and AM technology across the globe, crafting these lists of critical indicators likely cannot be a solo activity. Rather, further international coordination will likely be needed to understand the full impact of AM on the threat processes and to appropriately update indicators as a result.

MONITORING THE DIGITAL TO PREVENT THE PHYSICAL

In the past, if governments wanted to ban or control a new product, they could restrict the availability of that product either at its point of manufacture or at its point of sale. However, with AM, those two points can be variable: A product can be designed anywhere, sold digitally over the Internet, and manufactured anywhere where there is a suitable printer. This can present significant challenges for regulators and governments. Whatever method or material they use, all AM processes use digital information to fabricate physical objects.[42] Thus, if a government is to restrict the creation of certain types of AM products, such as automatic firearms or explosive triggers, they should do so across the whole supply chain—both digital and physical. To do so, there are two key avenues for threat intervention: along the physical supply chains, including the raw materials that are used to print, and the digital supply chains, including the design files or, as described in exports controls, technical data or technical information.

Steps are already being taken to control the physical supply chain, but none offer a full solution. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, for example, has unanimously adopted controls on certain AM equipment and software.[43] However, the inherent dual use of what AM can produce means that controlling the products of AM through regulation of the physical raw materials can be difficult. After all, the same plastic resin or metal powder can become a child's toy or an unregistered firearm. To help differentiate lawful uses from illegal or counterfeit products, taggants can be added to AM source material. But while this method can help to identify the source of a counterfeit or illicit product once it is made, it cannot preemptively stop its production.[44]

Therefore, these physical controls should be coupled with an expanded awareness of the digital side of the AM life cycle: examining how and where digital files are transferred, especially those files suspected for use as a weapon. Governments will likely need to identify, collect, and provide reporting on potential AM threats differently, in many cases while AM data remain in the form of digital files in cyberspace. By analyzing how and where traffic moves on the Internet and deep web, officials are better able to detect the unusual patterns of activity associated with the movement of illicit information to bad actors.

One cannot stop the technological advances—and opportunities—AM offers, but threats that arise must be thwarted as they emerge. This requires an intelligent understanding of what is possible, constant vigilance of the threat landscape, and coordinated action by affected state, local, federal, and international players. AM has the potential to bring boundless benefits to society, but to enjoy those benefits requires continuous vigilance.

ENDNOTES

1. Cyrus Farivar, *3D-printed gun maker now has federal firearms license to manufacture, deal guns*, Ars Technica, March 17, 2013, https://arstechnica.com/tech-policy/2013/03/3d-printed-gunmaker-now-has-federal-firearms-license-to-manufacture-deal-guns/.
2. Andy Greenberg, *3-D printed gun lawsuit starts the war between arms control and free speech*, Wired, May 6, 2015, https://www.wired.com/2015/05/3-d-printed-gun-lawsuit-starts-war-arms-control-free-speech/.
3. Ibid.
4. Adam Popescu, "Cody Wilson: The man who wants Americans to print their own 3D guns," *Guardian*, June 6, 2016, https://www.theguardian.com/us-news/2016/jun/06/cody-wilson-3d-guns-printing-firearms-lower-receivers.
5. Ibid.
6. For a full discussion of these dynamics, see Mark Cotteleer and Jim Joyce, *3D opportunity: Additive manufacturing paths to performance, innovation, and growth*, Deloitte University Press, January 17, 2014, https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-14/dr14-3d-opportunity.html.
7. Department of Defense, "Joint intelligence," *Joint Publication 2-0*, October 22, 2013.
8. Southern Poverty Law Center, *Lone wolf report*, February 11, 2015, https://www.splcenter.org/20150212/lone-wolf-report, accessed on May 2, 2017.
9. David A. Shirk, "The drug war in Mexico: Confronting a shared threat," *Council Special Report* 60, March 2011.
10. Virginia Page Fortna, "Do terrorists win? Rebels' use of terrorism and civil war outcomes," *International Organization* 69, no. 3 (May 2015): pp. 519–556.
11. Clare Scott, "Iran to host first additive manufacturing symposium in May," 3DPrint.com, March 10, 2017, https://www.3dprint.com/167554/iran-additive-manufacturing/; Clare Scott, "North Korean trade show advertises 3D printer . . . that looks a lot like a MakerBot," 3DPrint.com, June 3, 2016, https://3dprint.com/137135/north-korea-3d-printer/. last accessed on May 8, 2017.
12. Although this article focuses on the physical aspects of how AM can be used directly by malign actors to cause harm, it is nevertheless also important to recognize the potential indirect susceptibilities introduced by the friendly use of AM. Given that AM links the physical and digital worlds, making digital information real and tangible, it introduces a host of new considerations to many manufacturing decisions. Not least of these are cyber considerations: Digital inaccuracies in a design file or software can compromise physical devices, causing parts to underperform or even fail unexpectedly. For further information regarding digital risks in additive manufacturing, see John Brown, John Ezzard, Simon Goldenberg, and Jeff Haid, *3D opportunity in cyber risk management*, Deloitte University Press, August 23, 2016, https://dupress.deloitte.com/dup-us-en/focus/3d-opportunity/3d-printing-cyber-risk-management.html.
13. There are both federal firearms laws and state firearms laws. Under federal law, an individual need not obtain a license to make a firearm, nor must the gun be registered (18 U.S.C. Ch. 44 Section 922(d)). State laws vary and there are differing requirements on whether a license or permit is required to purchase or possess a firearm, register a firearm, allow for the concealed or open carrying of firearms, etc. (https://www.rt.com/usa/printed-3d-guns-ban-017/); Quora, "As an estimate, how many 3D printed guns are there currently?," https://www.quora.com/As-an-estimate-how-many-3D-printed-guns-are-there-currently; Sebastian Anthony, "The world's first 3D-printed gun," Extreme Tech, July 26, 2012, https://www.extremetech.com/extreme/133514-the-worlds-first-3d-printed-gun.

14. Thomas Campbell, William Cass, *3-D printing will be a counterfeiter's best friend: Why we need to rethink intellectual property for the era of additive manufacturing*, Scientific American, December 5, 2013.

15. Dawn Lim, *Counterfeit chips plague US missile defense*, Wired, November 8, 2011, https://www.wired.com/2011/11/counterfeit-missile-defense/.

16. Todd Halterman, "FBI to use 3D printing for bomb research," 3D Printer World, June 24, 2014, http://www.3dprinterworld.com/article/fbi-use-3d-printing-for-bomb-research.

17. As just one example, researchers at Raytheon have printed components for a small guided missile: Raytheon, "To print a missile: Raytheon research points to 3-D printing for tomorrow's technology," press release, March 19, 2015, http://www.raytheon.com/news/feature/3d_printing.html, accessed July 11, 2017.

18. Robert Kelley, "Is three-dimensional (3D) printing a nuclear proliferation tool?," EU Non-proliferation consortium, *Non-proliferation papers* no. 54, February 2017; Brookings, "Additive manufacturing builds concerns layer by layer," December 2015, https://www.brookings.edu/blog/techtank/2015/12/08/additive-manufacturing-builds-concerns-layer-by-layer/, accessed on May 8, 2017; "Communication received from the Permanent Mission of the Republic of Korea to the International Atomic Energy Agency regarding certain member states' guidelines for the export of nuclear material, equipment, and technology," IAEA information circular, guidance part 1, November 2016, https://www.iaea.org/sites/default/files/publications/documents/infcircs/1978/infcirc254r13p1.pdf, accessed on May 15, 2017.

19. Richard Parry, *The Bonnot Gang: The Story of the French Illegalists* (Oakland, CA: PM Press, 2016).

20. Mark Cotteleer, Jonathan Holdowsky, Monika Mahto, and John Coykendall, *3D opportunity for aerospace and defense*, Deloitte University Press, June 2, 2014, https://dupress.deloitte.com/dup-us-en/focus/3d-opportunity/additive-manufacturing-3d-opportunity-in-aerospace.html.

21. Kelley, "Is three-dimensional (3D) printing a nuclear proliferation tool?"

22. Brookings, "Additive manufacturing builds concerns layer by layer"; Popular Mechanics, "This chemistry 3D printer can synthesize molecules from scratch," March 2015, http://www.popularmechanics.com/science/health/a14528/the-chemistry-3d-printer-can-craft-rare-medicinal-molecules-from-scratch.html, accessed on May 2, 2017; the NSABB was charged with recommending a framework for the efficient and effective oversight of US federally funded dual-use life sciences research, considering both national security concerns and the needs of the life sciences research community.

23. Jim Joyce, Matthew Louis, and Tom Seymour, *3D opportunity for the department of defense*, Deloitte University Press, November 20, 2014, https://dupress.deloitte.com/dup-us-en/focus/3d-opportunity/additive-manufacturing-defense-3d-printing.html.

24. United States Department of Justice, *Overview of the law enforcement strategy to combat international organized crime*, April 2008.

25. In fact, the designer of the first 3D-printable firearm, Cody Wilson, filed a suit against the US state department on constitutional grounds in May 2015. For more information, see Alan Feuer, "Cody Wilson, who posted gun instructions online, sues state department," *New York Times*, May 6, 2015.

26. There are both federal firearms laws and state firearms laws. Under federal law, an individual need not obtain a license to make a firearm, nor must the gun be registered (18 U.S.C. Ch. 44 Section 922(d)). State laws vary and there are differing requirements on whether a license or permit is required to purchase or possess a firearm, register a firearm, allow for the concealed or open carrying of firearms, etc. (https://www.rt.com/usa/printed-3d-guns-ban-017/).

27. Quora, "As an estimate, how many 3D printed guns are there currently?"; Anthony, "The world's first 3D-printed gun."

28. Jack Karsten and Darrell West, *Additive manufacturing builds concerns layer by layer*, The Brookings Institution, December 2015.

29. Lawrence Livermore National Laboratory, *3D-printed foam outperforms standard materials*, April 29, 2016 (available on AdditiveManufacturing.com).

30. Cary Sublette, *Nuclear weapons frequently asked questions: Section 4.0 engineering and design of nuclear weapons*, http://nuclearweaponarchive.org/Nwfaq/Nfaq4.html, accessed July 11, 2017.

31. National Nuclear Safety Administration blog, KCNSC reaches milestone in digital manufacturing, October 7, 2016.

32. Kelley, "Is three-dimensional (3D) printing a nuclear proliferation tool?"

33. "The nuke detectives," *Economist*, September 5, 2015, https://www.economist.com/news/technology-quarterly/21662652-clandestine-weapons-new-ways-detect-covert-nuclear-weapons-are-being-developed.

34. Evan Perez, Jodi Enda, and Barbara Starr, "First on CNN: New terrorist laptop bombs may evade airport security, intel sources say," CNN, April 1, 2017, http://edition.cnn.com/2017/03/31/politics/terrorist-laptop-bombs-may-evade-security/index.html.

35. Connor McNulty, Neyla Arnas, and Thomas Campbell, *Toward the printed world: Additive manufacturing and implications for national security*, Defense Horizons, September 2012.

36. Brendan Koerner, *Why ISIS is winning the social media war*, Wired, April 2016.

37. The United Nations Office on Drugs and Crime, *The use of the internet for terrorist purposes*, September 2012.

38. The Department of Commerce, *Charter of the emerging technology and research advisory committee*, https://tac.bis.doc.gov/index.php/documents/pdfs/279-etrac-charter/file, accessed June 13, 2017.

39. Office of Bombing Prevention, Department of Homeland Security, *Counter-IED resources guide*, April 2014.

40. Department of Homeland Security, "Border enforcement analytics program apex infographic," accessed June 13, 2017.

41. Cynthia Grabo, *Anticipating surprise: Analysis for strategic warfighting*, Center for Strategic Intelligence Research, The Joint Military Intelligence College, December 2002.

42. Cotteleer and Joyce, *3D opportunity: Additive manufacturing paths to performance, innovation, and growth*.

43. For specific additions, see the Department of Commerce, *The Federal Register* 80, no. 98, part III.

44. Sharon Flank, Gary E. Ritchie, and Rebecca Maksimovic, "Anticounterfeiting options for three-dimensional printing," *3D Printing and Additive Manufacturing* 2, no. 4 (December 2015): pp. 180–189.

ABOUT THE AUTHORS

MIKE STEHN

Mike Stehn is a specialist master at Deloitte Consulting LLP's Federal Strategy and Operations practice. He brings almost 30 years of leadership and organizational management skills to Department of Defense and Intelligence Community clients. He is a retired army warrant officer and counterintelligence agent.

IAN WING

Ian Wing is a manager in Deloitte Consulting LLP's Strategy & Operations practice. He brings a decade of experience solving complex challenges for federal and military customers to bear on his client engagements. Wing's prior experience was in research and development at a major defense contractor, and he now focuses on helping clients realize business value and develop new capabilities with additive manufacturing and other advanced technologies.

TINA CARLILE

Tina Carlile is a senior manager in Deloitte LLP's Global Export Controls and Sanctions team in London. Carlile is a former US government international trade attorney with experience drafting, implementing, and complying with international trade law. She specializes in US munitions and dual-use controls. Prior to joining Deloitte, Carlile managed the US Department of Homeland Security's (DHS) export controls policy office. She led the development of DHS's internal export controls compliance program, served as the primary DHS representative to the President's Export Control Reform Initiative, represented DHS in Commodity Jurisdiction adjudications, and was DHS head of delegation to the Wassenaar Arrangement export controls negotiations.

JOE DICHAIRO

Joe Dichairo is a specialist leader in Deloitte Consulting LLP's Supply Chain practice. He has more than 26 years' experience in developing novel solutions to supply chain issues in the defense and national security arenas. Dichairo specializes in bringing emerging technologies such as additive manufacturing, IoT, and digital supply networks to bear on the military's most complex challenges. Prior to joining Deloitte, he was an officer in the United States Army serving as a combat arms officer, commander, and policy planner for the joint chiefs of staff.

JOE MARIANI

Joe Mariani, a manager in Deloitte Services LP, is series editor for Deloitte's research campaign on the Internet of Things. Mariani is responsible for examining the impact of Internet of Things on a diverse set of issues from business strategy to technical trends. His broader research focuses on how new technologies are put to use by society and the organizations within it.

ACKNOWLEDGEMENTS

The authors would like to gratefully acknowledge **Brenna Sniderman** of Deloitte Services LP and **Justine Bornstein** of Deloitte LLP for their advice and guidance throughout the development of this article.

CONTACTS

Kelly Marchese
Supply Chain Strategy leader
Principal
Deloitte Consulting LLP
+1 404 631 2240
kmarchese@deloitte.com

Bob Phelan
Managing director
Deloitte Consulting LLP
+1 571 882 7693
bophelan@deloitte.com

Stacey Winters
Aerospace and Defence sector leader
Partner
Deloitte LLP
+44 20 7007 0275
stwinters@deloitte.co.uk

Pablo LeCour
Global Export Controls and Sanctions
Partner
Deloitte LLP
+44 20 7303 8903
plecour@deloitte.co.uk

 Follow @DU_Press

Sign up for Deloitte University Press updates at www.dupress.deloitte.com.

About Deloitte University Press
Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.

Deloitte's Center for Integrated Research focuses on developing fresh perspectives on critical business issues that cut across industry and function, from the rapid change of emerging technologies to the consistent factor of human behavior. We uncover deep, rigorously justified insights and look at transformative topics in new ways, delivering new thinking in a variety of formats, such as research articles, short videos, in-person workshops, and online courses.