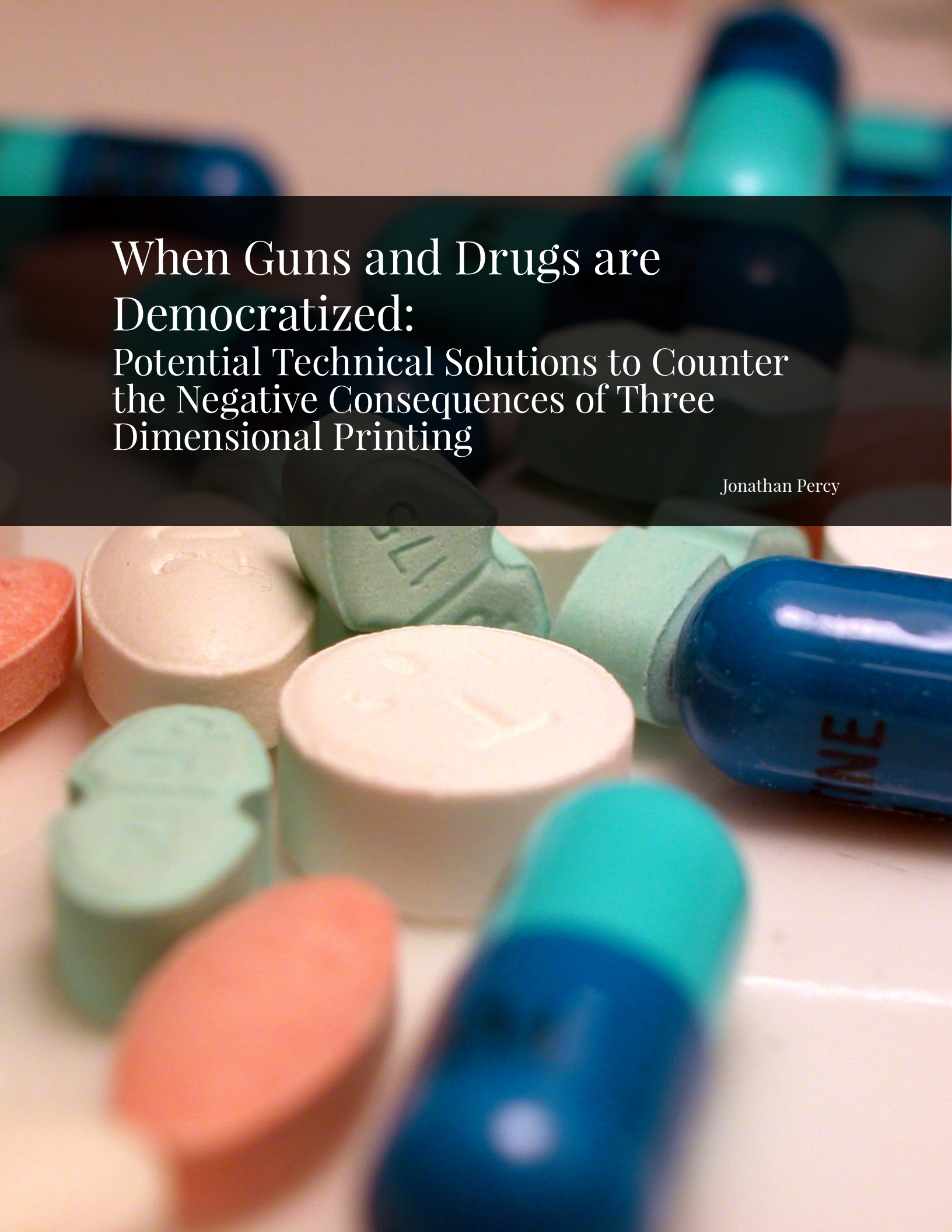

When Guns and Drugs are Democratized:

Potential Technical Solutions to Counter the Negative Consequences of Three Dimensional Printing

Jonathan Percy

Abstract

3-D printer technology will have negative consequences in the form of weapons that cannot be traced, illicit drug manufacture, sabotage, and intellectual property theft. This article poses the following questions. How will society be affected by these changes? How will border security organizations accomplish their missions when illicit guns and drugs no longer have to be transferred across borders? How might terrorists use their ability to hack design files to sabotage components built by 3-D printers? This article will focus on what can be done to limit, through the use of technology, the sinister uses of the 3-D printer while still allowing for the positive benefits that this new technology will bring to humanity. The article is structured to describe briefly how 3-D printing technology functions, how the technology can be used to print objects with negative consequences to society, and how those consequences may be remediated.

Suggested Citation

Percy, Jonathan "When Guns and Drugs are Democratized: Potential Technical Solutions to Counter the Negative Consequences of Three Dimensional Printing." *Homeland Security Affairs* 12, Article 7 (December 2016). https://www.hsaj.org/articles/13226

Introduction

The use of three-dimensional (3-D) printers is becoming more pervasive.[1] Researchers are revealing new objects that can be created using 3-D printing technology at a rapid pace.[2] In addition to inexpensive home-hobbyist printers that are capable of printing a multi-shot automatic gun, very sophisticated 3-D printers capable of printing human organs or military-grade weapons are in production.[3]

The use of 3-D printing technology may revolutionize how Americans shop, how medicine is manufactured, and how weapons are made. The benefits associated with 3-D printing technology may have far-reaching impacts for all of humanity. The global economy will change positively as 3-D printing becomes more pervasive, altering where and how objects are manufactured, how they are shipped around the world, and how they are distributed. However, similar to the Manhattan Project and the first use of nuclear fission, 3-D printer technology will have negative consequences in the form of weapons that cannot be traced, illicit drug manufacturing, sabotage, and intellectual property theft.

This article will focus on what can be done to limit, through the use of technology, the sinister uses of the 3-D printer. The article is structured to describe briefly how 3-D printing technology functions, how the technology can be used to print objects with negative consequences to society, how policy may be impacted, and how those consequences may be remediated.

A Brief Review of 3-D Printing Technology

"Computer: tea, Earl Grey, hot." With those words, fictional character Jean-Luc Picard introduced the concept of the Replicator on television's "Star Trek: The Next Generation" in 1987. Today, modern 3-D printing technology is beginning to realize the concept first envisioned by science fiction.

3-D printing, or additive manufacturing as it is also known,[4] refers to the production of a three-dimensional object through the layer-by-layer addition of material according to a geometric computer model.[5] The original patents for the technology date back to the late 1980s with numerous follow-on patents added as new materials and techniques were developed. 3-D printing is different than other forms of manufacturing that require either the removal or alteration, e.g., molding or extruding, of material to produce a completed object.[6]

An example of how 3-D printing creates an assembled product as opposed to a set of parts that still require assembly was described by McNulty, Arnas, and Campbell in Defense Horizons:

> *Instead of using cutting tools to machine desired shapes from blocks of metal and then assembling those parts into a completed tool, a 3-D printer could build a crescent wrench by adding a layer of material and stacking another layer on top of that one and fusing them together, repeating the process until the wrench is complete. Additionally, since the wrench is not assembled from preexisting parts, it would be a complete entity—unable to break into component parts as there is only one 'part.' Since the wrench is made by additive manufacturing as opposed to conventional 'subtractive manufacturing'—taking a block of raw material and removing excess until the finished product remains—the process as a whole is more efficient and less wasteful.*[7]

The use of the 3-D printer as described above yields a finished product ready to be used immediately off of the printer instead of waiting for a completed assembly.

The 3-D printer receives its instructions via a software program generically called computer aided design (CAD). The CAD system models the desired object in a solid-modeling program, which means that its models are an agglomeration of points in space rather than a hollow group of stitched-together polygons. With its emphasis on solid, volumetric materials, this type of modeling is particularly well-suited for 3-D printing.[8]

After designing the desired object to be manufactured using the CAD program, a design file in a format called Stereolithography (STL) is sent to the 3-D printer. An STL file renders surfaces in the CAD design as a mesh of triangles. The number and size of the triangles determine how accurately curved surfaces are printed.[9] The 3-D printer interprets those STL files into layers, so the object can be built up by the additive printing process.

There are currently seven printing technologies that are in broad development: binder jetting, directed-energy deposition, material extrusion, material jetting, powder bed fusion, sheet lamination and vat photopolymerization.[10] This article will not address the different technologies employed by those methods, but it is important to note that they all employ a technique that adds material to a previously deposited layer. Hereafter, for the purposes

of this article, the many different techniques for 3-D printing of objects have been grouped under the single descriptor, 3-D printing. 3-D printer technology has expanded, so it can print a variety of materials. Appendix 1 lists the many types of materials that may be printed by 3-D printers.

Because there is an assortment of materials that can be manufactured via 3-D printing, the technology has become attractive for a wide variety of manufacturing purposes. One of the leaders in 3-D printing technology is the Cornell Creative Machines Lab. Its Director, Mr. Hod Lipson, is looking beyond near-term advances in 3-D printing and is trying to stay ahead of the curve. He postulates that the field of electronics printing will bring 3-D printing technology to the next level. Lipson described where his team is moving next with their research, "we're spending time on electronics printing, active systems, and, in particular, voxels (3-D pixels)." Lipson explains that embedding electronics and prefabricated components into conventional 3-D printing will move the technology toward the creation of integrated systems.[11]

3-D printing of organic objects and even complex jet engines is happening today. General Electric recently demonstrated a functional jet engine that was built entirely from 3-D printed parts.[12] The technological breakthroughs in the field are being made at an exponential pace, so much so that it is exceeding the pace predicted by Moore's law.[13] Any discussion of 3-D printing becomes obsolete nearly before it is published.

Unfortunately, criminals and terrorists are very often early adopters that use technologies for illicit purposes not originally intended by the inventors and innovators. A review, then, is necessary to examine how the 3-D printing technology may be misused by criminals and terrorists.

Opportunities for the Misuse of 3-D Printing

Cyber-crime has been associated with the Internet since its growth beyond research and military institutions.[14] To date, most of that crime has been perpetrated in the realm of financial and intellectual property data and information. With 3-D printing technologies, cyber-criminals and terrorists can affect the constructed three-dimensional world by simply manipulating the binary code that instructs the printers what to print. It is believed that while still in the infancy of 3-D printing technology, the time is right to discuss the potential pitfalls of 3-D printing and to initiate preventive measures and policies to ensure that the technology is used for good rather than for criminal intent. There are many opportunities for illicit use of 3-D printing technology: printing of controlled substances, manufacturing of weapons that are untraceable, stealing intellectual property and use by competitors, and purposeful sabotaging of competitor's designs. All of these scenarios provide opportunity for bad actors to use this technology for crime or terrorism.

Currently, two of the world's three largest illicit trades are drugs and arms; the third being the illegal harvesting of endangered species. Drugs are by far the biggest category, accounting for slightly less than one percent of global commerce or $321.6 billion dollars a year, according to a 2003 UN report.[15] The Small Arms Survey estimates that illegal trade accounts for roughly 10 percent of the Arms market and accounts for perhaps two billion dollars annually. Terrorists and criminals can make large sums of money on the trade of

these items because society has made it illegal to openly trade these goods through unofficial channels. Governments often target specific organizations that are avowed enemies of the state to limit their access to illegal substances and arms. 3-D printing offers a new tool to terrorists and criminals attempting to circumvent the limitations placed upon them by governments.

Printing Pharmaceuticals

Printing pharmaceuticals became commercialized in August, 2015 when the U.S. Food and Drug Administration approved the first 3-D-printed pill: spritam levetiracetam, a drug that can reduce seizures among epileptics. Manufactured by American pharmaceutical company Aprecia, it is produced not by a tableting machine but by a special process in which the drug's active and inactive ingredients are laid down layer-by-layer. This unusual manufacturing technique helps Spritam's patients in particular. By building each dose individually, Aprecia says it can make each pill more porous and more potent than more traditional techniques allow. Pills printed through the company's special process "disintegrate [orally] in less than 10 seconds," Aprecia explains, which is unusually quick for a high-dose drug.[16] The use of 3-D printing has improved the efficacy of the drug because of the manufacturing process which will add a new economic variable to the pharmaceutical industry by improving drug performance instead of having to discover new drug compounds.

In a 2012 TED Talk, Lee Cronin of the University of Glasgow described a new approach to 3-D printing that could enable patients to print their own medicines at home. What's needed, he explained, is a universal set of "chemical inks" as well as a way to 3-D print the lab instruments and these chemical inks at the same time. In essence, this would let 3-D printers catalyze the chemical reactions to print drugs when needed. As a result, the pharmaceutical industry could eventually witness a transition from filling prescriptions to providing algorithms for the drugs. Doctors could hand off an algorithm to a patient to go print at home on a 3-D printer rather than jotting down a prescription on a piece of paper. These algorithms would include information about the set of chemical inks needed to print the medicine as well as the molecular blueprints.[17] When commercialized, printing of drugs at home will place the tools to print any drug compound into the privacy of the home and out of the view of regulatory agencies.

Personalized medicine creates an approach whereby each patient is treated based on his or her precise genetic makeup. The National Institutes of Health (NIH) defines precision medicine as an emerging approach for disease treatment and prevention that integrates an individual's variability in genes, environment and lifestyle. Precision health may be the secret to predict and ultimately prevent various diseases already present in the inner workings of our genetic profile.[18]

A new era is beginning where drug ingredients are punched into a 3-D printer wired with a set of chemical inks. Known patient allergies are preprogrammed into the 3-D printer to avoid negative reactions to medications. In the future, pharmaceutical drugs created at home will eliminate the ingredients to which the patient is allergic but keep the ones needed.[19] There are downsides to 3-D pharmaceutical printing, including illegal drug manufacturing, mislabeling, and cybersecurity concerns. Regulators and the pharmaceutical industry will have to work together to keep illicit activity at bay.[20]

Along with the potential benefits of personalized medications that match an individual patient's genome, the opportunity for misuse of those pharma- printers is also significant.[21] With the proper set of chemical inks, a 3-D printer can be programmed to produce methamphetamines, cocaine, and Oxycontin.[22] Law enforcement will have to adapt quickly to the new dynamic of drug abusers who print their own drugs instead of buying them through the established methods of the past. The possibility of illegal drug abusers experimenting with their own drug cocktails will also become easier with the 3-D printer. As amateur chemists develop new compounds to get to that next new high, the potential consequences of users trying out new compounds may prove fatal. As an example, users of an illegal drug known as K2 continue to use it despite known hazards.

> *Once the original K2 chemical compounds were banned on the federal and state levels, entrepreneurs both overseas and homegrown began to tweak the formula – named JWH for its creator, chemist John Huffman. These later versions created vaguely the same effect (as marijuana), but police have been stymied in their ability to make arrests if the molecular structure of the substance varies by even a hydrogen atom from that outlawed by legislation. K2-induced side effects, which can include vomiting, high blood pressure, and even seizures and hallucinations, have caused a sudden, alarming rise in trips to local emergency rooms.*[23]

Despite the known hazards of K2, amateur chemists continue to produce it and desperate people continue to buy it.

Every year, Texas Department of Public Safety and U.S. Customs and Border Patrol agents catch hundreds of drug runners, called mules, and confiscate thousands of pounds of illegal drugs crossing the Mexican border. The need to smuggle contraband across the border will lessen with the advent of 3-D printers capable of printing illegal drugs. Before that fear becomes a reality, the chemistry must be digitized so that a blueprint for the molecules directs the printer to build the illegal drugs from scratch.

Glasgow University chemist Lee Cronin explained it:

> Nearly all drugs are made of carbon, hydrogen and oxygen, as well as readily available agents such as vegetable oils and paraffin. With a printer it should be possible that with a relatively small number of inks you can make any organic molecule.

Cronin's idea is to make prescription drugs downloadable; however, when actually built, Cronin's "chemputer" could make illicit drugs available to anyone, in whatever quantity and quality desired.[24]

It is unclear how homeland security and law enforcement will mitigate these problems before they begin. David Hodgson, partner in Deloitte's healthcare and life sciences team says, "The current global, regional and local regulatory environment is incapable of accommodating the ambiguity of a 3-D printing process." Untangling whether regulatory efforts should target the printer, the ingredients used by the printer, or the person doing the printing becomes an important question.[25]

One method for ensuring that illegal drugs cannot be printed is to control the drug blueprints accepted by the printer as a valid print file. Manufacturers could program 3-D printers to accept only a set of encrypted drug templates, which would ensure that only legal and

approved drugs could be printed. An additional check set into the printer's firmware would match a blueprint queued up for a print job against a known set of unacceptable chemical compounds. If unacceptable compounds were detected in the print file then the printer would not execute that print request. In order to accomplish a solution similar to what is described above, it is necessary to produce legislation that would require 3-D printer manufacturers to create those checks before initiating a print job. Furthermore, there is a need for a private or government consortium that would hold a library of legal drug blueprints that a printer would validate against before initiating the print job.

Untraceable Weapons Manufacture

Probably the most widely publicized potentially negative consequence of 3-D printing is the printing of untraceable firearms. Opponents of strict regulation of 3-D firearm printing claim that printing a gun is not just making a weapon; it is also making a free speech argument. It is an argument that combines the act of gun-making with an ideological challenge about freedom of information and file-sharing.[26] In countries such as Japan, the United Kingdom, and Australia where there is strict gun control, people may choose to print weapons as a way around those controls.

Cody Wilson, a self-described "crypto-anarchist," said,

> The Internet and cryptography are these anarchic tools that can allow for the expanse of citizen action. We like the idea of the market becoming completely black and starving the nation-state from all the money they claim.[27]

Cody Wilson's nonprofit organization, Defense Distributed, released a video showing a gun firing off over 600 rounds—illustrating what is likely to be the first wave of semi-automatic and automatic weapons produced by the additive manufacturing process.

The assault rifle model number AR-15 is designed to be modular, meaning it can receive different types of "uppers" (barrels) as well as different-sized magazines. "This is the first publicly printed AR-15 lower demonstrated to withstand a large volume of .223 ammunition without structural degradation or failure," Wilson writes. "The actual count was 660+ fired on day one with the 3-D printed lower. The test ended when we ran out of ammunition, but this lower could easily withstand 1,000 rounds." Already, he says, over 10,000 people have downloaded the lower CAD file, and more have downloaded it through BitTorrent.[28]

In May 2013, Wilson also designed the Liberator, the world's first fully 3-D printed plastic gun, designed to fire standard .380 handgun bullets, and 100,000 people around the world downloaded the drawings. When asked by the press how he felt about his accomplishment, Wilson replied that now "anywhere there is a computer and an Internet connection, there is a promise of a gun."[29]

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) produced its own version of the Liberator. "We downloaded files, we created firearms from those files, and we tested those firearms," Earl Griffith, chief of ATF's firearms technology branch, said in a briefing with reporters at ATF headquarters in Washington. The ATF's testing showed that the weapon, while not quite as powerful as most guns, could penetrate several inches of soft flesh as well as a human skull. The Liberator can only fire one shot before it must be reloaded, but ATF officials noted that's all a determined assassin needs.[30]

The design of the Liberator includes a block of metal that technically makes it legal under the Undetectable Firearms Act, which requires that a certain amount of metal be included in a weapon so it is detectable.[31] However, the metal plays no role in the weapon's function and could be easily removed.

It is worrisome that technology is now available to anarchists and terrorists to print weapons that cannot be traced by authorities and that can be produced in the privacy of a personal workshop. In history, the ability to covertly manufacture weapons has been available to the skilled machinist; however, the required skill to accomplish the manufacture of an untraceable weapon has dropped dramatically with the advent of 3-D printer technology.

The ability to 3-D print guns privately will allow individuals to bypass background checks, the primary way that guns are regulated. Today, licensed firearms dealers conduct background checks and ensure that they sell only to people legally eligible to purchase. President Obama's 2013 gun-control proposals[32] included not only more restrictions on who is permitted to buy and own guns, but also called for private sellers — who today don't have to run background checks — to sell instead through licensed dealers. The relevance to 3-D printing is that a person can avoid the intent of the regulation process by printing a gun instead of buying it from a licensed gun seller.

According to today's federal law,[33] an individual may purchase a long gun (rifle or shotgun) at age eighteen and a handgun at age twenty-one, as long as the purchaser has not committed a significant crime, is not mentally ill, and is a citizen. It is not possible, however, to enforce the above regulations when individuals print weapons at home. With no seller, who will run background checks or deny purchases? The government's control mechanisms become moot.

The lower, or "lower receiver" portion of a firearm, is the crucial part that contains all of the gun's operating parts. Under American law, the lower is what is defined as the firearm itself and is what is registered with the Federal government.[34]It holds together the stock, the grip, the ammunition magazine, and the upper receiver, which includes the barrel and the chamber where the cartridge is detonated. As Doug Wicklund, senior curator at the National Rifle Association museum explained, the lower receiver always has carried the serial number because it's the part that remains when the others wear out and are replaced. Like the frame of a bicycle or the motherboard of a computer, it's the nucleus of the machine around which everything else is constructed.[35]

With the advent of 3-D printing, the gun's lower receiver can be produced with no unique identifier and no trail leading back to the manufacturer. This creates the opportunity for anyone to print a gun in the privacy of their home without fear of the weapon ever being traced back to them.

3-D printed guns pose a problem for homeland security and law enforcement officials because the weapons produced by printing are unlikely to be caught using traditional investigative methods. As an example, the US border protection system catches thousands of weapons and tons of ammunition each year at US Ports of Entry between Mexico and the US.[36] The possibility of losing weapons that are detected at border checkpoints would no longer be a problem for terrorists and criminals if they can print their weapons once they have reached their destination.

Technology may once again be employed to help with the potential problem of untraceable weapons. The designs of lower receivers have some common elements that can be screened for by the 3-D printer. Since ammunition comes in standard sizes the dimensions of components that hold the ammunition, such as magazines and the chamber, can be checked for in an incoming design. The printer could be designed such that a specific code must be entered into it before it will print an object that has the dimensions or functionality similar to that of a lower receiver. The printer user would receive that code by registering for it with the Bureau of Alcohol Tobacco and Firearms (ATF). Upon entering the code, the 3-D printer would be permitted to print the part and the code would also be printed on the part.

This kind of a solution has a very broad impact. A new system of registering receivers to 3-D printers would be required at the ATF. The 3-D printer designs would become more complex to add the checking algorithms and the registration software. This would not stop a user from grinding off the serial number, but it would register the original manufacture of the receiver. Printer manufacturers, motivated by profit margins, are unlikely to add this additional complexity unless legislation is passed that requires them to do so. Further, the ATF will not create the registration process unless legislation is passed that requires them to do so. Regardless of how difficult the policy changes may be to register weapons manufactured using 3-D printers, it is technically achievable to identify a lower receiver print job. The policy changes will prove to be much more difficult to achieve than the technical changes. Gun lobbies will object to attempts by the Government to control 3-D printed weapons. Politicians will be under significant pressure by their constituents to stay away from the issue. It is beyond the scope of this article to address that issue; however, meaningful protection against 3-D printed guns will only occur if politicians have the courage to move past the lobbyists and address new policy.

Intellectual Property Theft

The Intellectual property (IP) protection challenge related to 3-D printing has gained visibility as the technology emerged from prototyping and began to produce objects and products from a broad range of materials. As defined by the National Crime Prevention Council,

> *IP is any innovation, commercial or artistic; any new method or formula with economic value; or any unique name, symbol, or logo that is used commercially. Intellectual property is protected by patents on inventions; trademarks on branded devices; copyrights on music, videos, patterns, and other forms of expression; and state and federal laws.*[37]

IP is a critical asset to the U.S. economy and to national security. In 2013, Gartner[38] predicted that by 2018, 3-D printing will result in the loss of at least $100 billion per year in IP theft, globally.[39] To date, very few technical solutions that address this challenge have appeared on the market.[40]

IP theft has been a significant problem across the Internet. A thief steals IP by accessing and copying another's ideas or product design. Thieves can reap huge profits by putting the original idea into production before the originator has done so. IP theft can damage the reputation of the original maker of the counterfeited product, cause the loss of competitive advantage, and risk national security.

Much of the world's problem with intellectual property theft can be traced to one country: China. Eighty-five percent of the counterfeit goods seized in the European Union in 2010 were believed to have come from China. Almost eight percent of China's gross domestic product comes from counterfeiting creative works, consumer goods, industrial products, and software.[41]

The scope of IP theft in the U.S. is significant. In the United States, the 14,841 seizures of counterfeit goods and unlicensed knockoffs had a domestic value of more than $260 million and accounted for 76 percent of all counterfeit goods.[42] In testimony to the U.S. Congress, FBI Assistant Director of the Counterintelligence Division, Randall C. Coleman stated:

> *Our foreign adversaries and competitors are determined to acquire, steal, or transfer a broad range of trade secrets in which the United States maintains a definitive innovation advantage. This technological lead gives our nation a competitive advantage in today's globalized, knowledge-based economy. Protecting this competitive advantage is vital to our economic security and our national security.*[43]

As 3-D printing becomes more of an integral practice within manufacturing, thieves will focus on stealing the stereolithography (STL) files. With the STL file, the thieves will have not only the appearance and dimensions of a component but also clear identification of the materials used, the tolerances selected and the means for assembly. In addition to facing the loss of their IP, victims will potentially lose the race to first distribute their products to the market.

IP can be stolen from a 3-D printer as described in a National Institute of Standards and Technology paper published in 2014:

> *Many replication devices use nonvolatile storage media to manage jobs and control the device. Potentially all of the information that was ever processed, stored, or transmitted by the device could remain in the nonvolatile storage indefinitely. Nonvolatile storage media for replication devices is most often in the form of a hard disk drive or solid state drive. Some replication devices may also provide for the use of removable solid-state memory cards. Information stored within a replication device may leave organizational information open to numerous exploits and compromises of confidentiality or integrity.*[44]

The use of nonvolatile storage within a 3-D printer leaves it potentially open to hacking threats via a network attack. When 3-D printers are not protected by appropriate security controls, information stored on the device becomes vulnerable to hackers attempting to gain access to the IP stored on the machine.

As noted in the NIST paper referenced above, some of the common threats to all digital equipment connected to the internet, which includes 3-D printers, are shown in Figure 1.

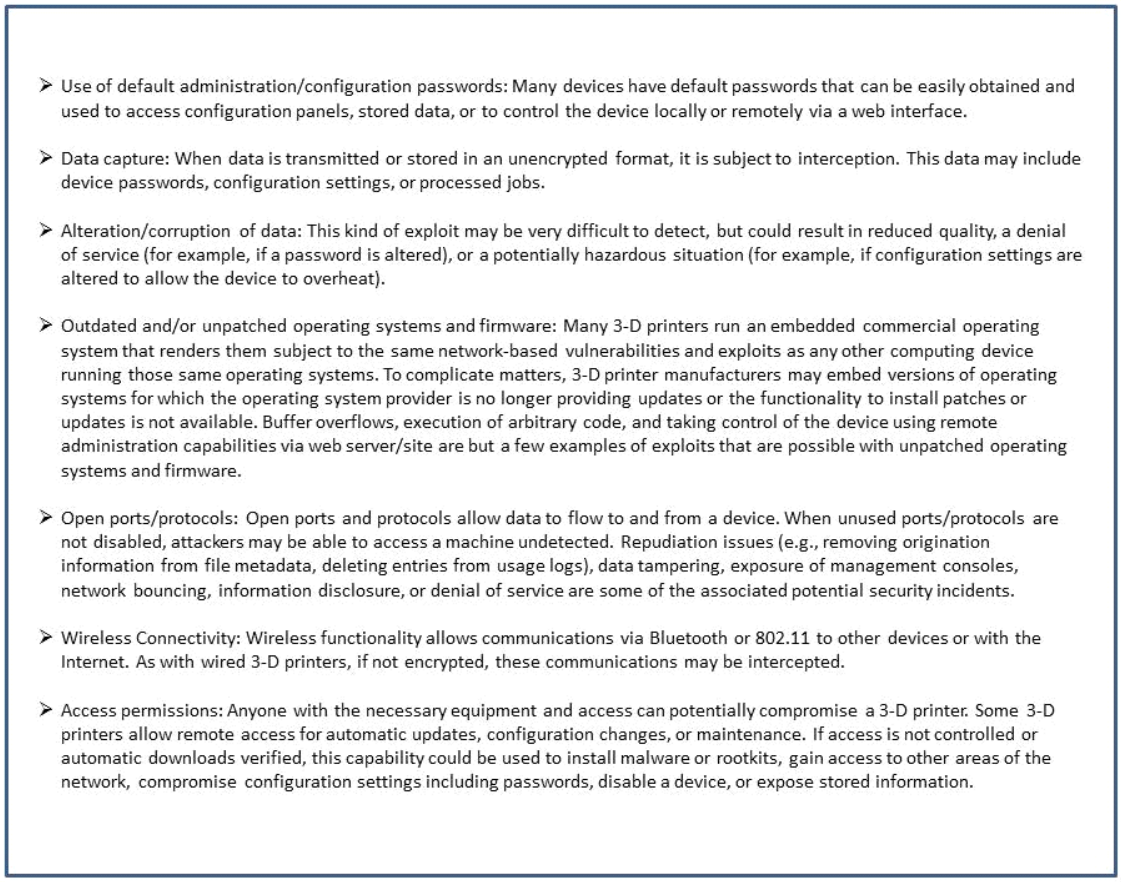

Figure 1. NIST Guidelines to Secure Data Integrity

Although the cyber threat to 3-D printers is not unique to these digital devices, the threat is no less pernicious because it is well known. Many new technologies are derivatives of other technologies that may have more mature controls around them. Often, however, those mature controls don't migrate to the new technology immediately with potentially deleterious effects.[45]

IP protection can be addressed from multiple perspectives. Some key perspectives are: (1) securing content such as 3-D models, which are used to create 3-D prints; (2) creating markers on the objects that authenticate those objects; and (3) search engines that compare 3-D objects.[46]

Gartner recommends that clients implement digital asset management and product data management software to control access to digital content, which is the source 3-D data needed to create 3-D prints. Those responsible for protecting enterprise IP should also monitor the market for vendors that embed markers on 3-D prints. For example, Applied DNA Sciences promotes its use of DNA to mark genuine products with visible or invisible signatures that, when screened, identify the product as genuine. This is a feasible approach, although Applied DNA Sciences is not yet widely known, nor is the technique proven on a significant scale.

3-D geometric search technology (such as that available through Geometric and Siemens PLM Software) shows promise in detecting the illegal use of content to print counterfeit

parts.[47] The search engines can compare 3-D models to print against other 3-D objects that the search engine might find on the Web. When matches across 3-D models are sufficiently close, a suspect model might be identified for further review. While such technology is in the early adoption phases for sourcing parts, an extension to IP protection is a possibility.

Enterprises either will redefine their business strategies to reduce the potential impact of IP theft, or introduce steps in the manufacturing to ensure that original and replacement parts are not counterfeit. Some 3-D printer manufacturers may emphasize value-added security services that protect against the theft of IP or sabotage of stereolithography (STL) files, rather than prioritizing the physical creation of products as their key value proposition. DNA marking or alternative processes will increasingly become an integral part of creative processes. Implementation of IP protection practices will lengthen design, R&D and manufacturing processes. This is likely to increase the costs of designing, producing, sourcing and maintaining products.[48] Implementation of value-added security services may put manufacturers at a competitive disadvantage when competing against unscrupulous producers; however, customers who value legitimate goods and who are fearful of possessing stolen goods will demand legitimate products.

Sabotage

Using similar attack methods as those described for the theft of IP, criminals or terrorists could choose a more malevolent approach and sabotage the component being printed by a 3-D printer. Although this is a much more complex attack than the more simple IP theft threat, the STL file could be altered by the attacker to change key structural components so they would not function as originally designed. As an example, the structural bulkhead components that are made by a 3-D titanium printing process for BAE's[49] Typhoon fighter-bomber could be adversely impacted by sabotaging the print file.

These aft end components provide critical structural support for the engines as well as for the vertical and horizontal stabilizers. If the 3-D STL file were altered to change the metallurgic properties of the titanium as it was being deposited, or if the webbing were made more porous than originally designed, the structural consequences could be catastrophic.

Similar sabotage can be envisioned for the printing of vaccines. An organic pathogen could be introduced into the original vaccine's STL file resulting in a harmful poison. Unless 100% quality control measures were taken to test for such pathogens, they could remain undetected until people fell ill from the introduced toxin.

Although sabotage to military jet components or to vaccines can happen now, the real danger to products being created via 3-D printing is that they all are being created from an original binary data file composed of ones and zeros. A saboteur doesn't have to physically attack an object in order to damage its original purpose; instead, the attacker merely alters a computer file, and the 3-D printer does the work for him. The attacker doesn't even have to be in close proximity to the object being sabotaged – he or she can attack from half a world away.

The other danger from sabotage is loss of productivity. Unless STL files are checked for validity before the printer begins its work, a sabotaged file will enable the device to print an unintended object--resulting in lost time and resources. That has already been demonstrated

by the STUXNET worm[50] when it specifically infected a certain make and model of high-speed centrifuges. Although the Siemens centrifuges are not 3-D printers, the controller logic is very similar. The attack achieved its desired effect of slowing the enrichment of Uranium by the Iranians. An attack by terrorists could have a similar desired result of slowing the production of objects critical to a U.S. project.

PMC Group President Michael Chipley confirms that 3-D printers attached to a network present a danger to the manufacturing industry; "a weakened printed part that makes it into an assembly line, or even worse, out to a delivered system or product" could be very dangerous. Chipley, who is an expert on cyber security, concurs that the NIST report was valid, stating that unsecured 3-D printers connected to the internet could be an easy target for spies or terrorists.[51] The subtle difference of a sabotaged part made from 3-D printing versus a sabotaged part made through a traditional machining method is that the sabotage can be done by a saboteur operating remotely instead of a saboteur working directly with the manufacturing machine, completely changing the security paradigm.[52]

A saboteur could implement the act of sabotage by changing the pattern of ones and zeroes that comprises the CAD of an object. To prevent that act, the system must detect the pattern change by comparing the received STL to the original design of the object.

A process to confound sabotage means additional steps in the programing of the 3-D printer. Today, a 3-D printer receives an STL file and adds it to its queue for execution. To obviate sabotage, a step needs to be added to check the STL files against the original CAD file to ensure that nothing has been altered. This additional step may be accomplished through a number of techniques. As an example, a "checksum"[53] value may be added to every word of computer instructions sent to the 3-D printer. The printer would calculate a checksum value of the instructions it has received and compare it to the checksum value from the original CAD file, and if it did not match, the printer would know that the file had been altered. Alternatively, the STL file can be encrypted by the originating CAD system and decrypted by the printer. A saboteur would have to decrypt a file first in order to sabotage it, which is difficult to accomplish with today's encryption algorithms.

Of course, a saboteur could alter the CAD file in the original design software before the STL file is sent to the printer. This gets into cyber security issues which are not a part of this article; however, available literature is rich with content regarding the detection and mitigation of cyber-attacks.[54] To be sure, the cyber warfare environment is a continuous arms race and keeping CAD software application and operating system software current with the latest versions is the best protection against evolving threats.

To date, 3-D printer manufacturers and CAD system developers have not incorporated the additional checks into the design of their systems and are unlikely to do so until legislatively mandated. Instead, the focus for 3-D printer manufacturers has been to decrease their costs while maximizing their product's features.[55]

Homeland Security Implications

Mandating that 3-D printers not be used for illicit purposes will have little to no effect on how they may be used by individuals determined to print illegal objects. The consequences of 3-D printing for homeland security organizations are broad and deep.[56] Numerous

organizations may be impacted by the illicit use of 3-D printers by criminal and terrorist organizations. The Drug Enforcement Agency (DEA) and Customs and Border Patrol (CBP) organizations will encounter significant challenges when drugs can be printed closer to the end customer. Both organizations employ significant resources to try and stop the flow of illicit drugs close to production of the drug rather than at the final retail distributor. They employ that strategy in order to try and eradicate the drug flow closer to the drug kingpin as opposed to stopping the low-level drug pusher. However, if the low-level drug pusher also becomes the producer then interrupting the supply chain will no longer be an effective means for interdiction. One could argue that instead of interdicting the flow of illegal drugs, the DEA and CBP will interdict the constituent chemicals. But if the constituent building blocks are carbon, hydrogen and oxygen there is no way those elements can be controlled.

Printing of mostly plastic guns with only small amounts of metal included will make the use of magnetometers much less effective as a detection method. The Transportation Security Administration (TSA) will have to change their screening methods if plastic guns become more broadly introduced into society. Law enforcement organizations and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) will have to change the means through which they try and regulate arms. Registration efforts are centered on the sale of weapons from licensed dealers. Background checks of prospective purchasers are conducted with the anticipation that people who should not legally possess a gun are stopped before the purchase is completed. That process is circumvented with the advent of 3-D printers that produce guns. Law enforcement will have no way to trace gun ownership. There will be no method for determining the extent of the number of guns on the street. Weapons created by 3-D printers and recovered at crime scenes will have no owner provenance. As the 3-D printer evolution continues, printing of ammunition will also be possible, thus rendering moot the concept of control of guns via control of ammunition.

It is currently legal to 3D-print guns, and it will remain legal until lawmakers make laws that make it illegal. The ATF is not a policy-making agency, so they cannot enforce a law that does not exist. Americans create technology much faster than lawmakers can regulate it. That can be a positive thing; in this case, however, it's a dangerous one. As Cody Wilson said when he created the first 3D-printed gun, "I recognize that this tool might be used to harm people—It's a gun."[57]

Intellectual property (IP) theft via 3-D printing will pose significant problems for the Federal Bureau of Investigation, Immigrations, Customs Enforcement and the judicial system. Anti-counterfeiting campaigns have long linked counterfeit products to organized crime and terrorist groups, but this has not yet proved compelling to consumers – one reason being the lack of evidence (or rather the publication of such evidence) linking the two. Dennis S. Prahl, a lawyer at Ladas and Parry comments: "I would hope that the message that trademark counterfeiting is strongly linked to terrorist and organized crime activities will gain traction in the public consciousness, but until al Qaeda is actually linked to fake handbags or watches in some raid, the media may not catch on to this story."[58]

Proving what is authentic and what is fraudulent will become problematical unless genuine objects are created with authentication markers that can't be replicated by forgers. Further, the provenance of the 3-D printed object is difficult when anyone with a printer and the right materials can duplicate an object. The FBI and local law enforcement organizations will need to expand their cyber units to accommodate the increase of investigations resulting from the additional theft of IP via the use of 3-D printers.

The FBI and private industry will both be affected as they employ resources to search for and stop sabotage implemented via 3-D printing. The National Security Agency (NSA) will also be impacted as they will be enlisted to try and determine if sabotage was initiated by foreign actors. Since sabotage may be initiated by a nation attempting to foil the production of a national asset or by a company trying to maintain a market share by disrupting its competition, law enforcement as well as the Intelligence Community (IC) will be employed to try and identify the perpetrator of the sabotage.

The above examples merely scratch the surface of how the homeland security community may be affected as criminals and terrorists expand their use of 3-D printers. Standard operating procedures used by Government agencies will require change to meet the new threat. Expensive technologies developed and deployed to catch the movement of illegal objects at borders and airports will be rendered useless since guns and drugs can be printed at the terrorist's or cartel member's destination. Industry must create new technologies, and government must create new laws to allow for interdiction of undesirable STL files.

Conclusion

In 2014, Congressman Steve Israel (R-NY) introduced legislation that would fully ban 3-D guns. Although it did not pass, he plans to reintroduce legislation that would once again ban 3-D guns and all plastic firearms. Israel argued: "[m]y legislation is about making sure that we have laws in place to ensure that criminals and terrorists can't produce guns that can easily be made undetectable. Security checkpoints will do little good if criminals can produce plastic firearms and bring those firearms through metal detectors into secure areas like airports or courthouses."[59]

Can successful legislation against the use of 3-D printers, programed to print objects that would be considered undesirable by American society, be passed into law? Laws could be created but would be largely unenforceable. In the case of weapons[60], even though legislation currently exists mandating that a gun must be registered to someone legally permitted to own a gun, most weapons used in a crime have been obtained illegally.[61] Instead, other technological solutions must be considered in order to prevent, or at least track, the printing of objects deemed socially undesirable.

Since two of the world's three largest illicit trades are drugs and arms, the 3-D printer will provide a new tool for organized crime to use as they manufacture goods to traffic in those trades.

Organized crime has benefited from the control of illicit goods by governments and by trafficking in black market products. Their near monopolies have allowed them to control the nearly two trillion dollar annualized trade in illicit goods. But what happens to their business model when guns and drugs are democratized? The advent of 3-D printing of drugs, organic materials and weapons provides the potential for much easier access to illegal drugs and untraceable weapons.

Considering the size of these illicit trades and the amount of money that criminals now make from them, organized crime will react to the threat that 3-D printing will have on their business. One thing the world has yet to see is what happens when the Mexican drug cartels declare war on a technology while simultaneously using the technology for their own

nefarious purposes.[62] This article has shown that technological means can be employed to control the production of undesirable products through the use of 3-D printing. Those technological solutions (or something like them) should be employed so that society can realize the potential benefits that 3-D printing offer while controlling the negative consequences that may accompany the wide-spread adoption of 3-D printing.

Legislation will not be enough to stop the 3-D printing of illicit items; however, legislation can and should be enacted to require manufacturers of 3-D printers to install encrypted templates for weapons, illicit drug compounds and trademarked designs so that the printer will not print objects that correspond to one of those protected templates. Much like current anti-virus software, the templates will have to be continuously updated to stay current with illicit designs, but that kind of solution would put teeth into legislation that prohibits 3-D printing of illegal material.

Although there is no evidence that terrorists have used 3-D printers in their actions to date, that is not a reason to assume that they never will. Leadership in homeland security and law enforcement should not ignore the potential illicit use of 3-D printers until those problems have become real – action to employ technical solutions should be taken now while the industry is still young.

About the Author

Jon Percy is the former Chief Information Officer and Assistant Director of Information Technology at the Texas Department of Public Safety and currently serves at the Texas Department of Health Services. He is the former Vice President of Homeland Security and Cyber at Textron Systems, Inc. He is currently enrolled as a student in the Center for Homeland Defense and Security at the Naval Postgraduate School. He has an abiding interest in technology and how it can best be used in the fight against terrorism. Mr. Percy has spent much of his career in support of the Intelligence Community and has developed products that turn data into actionable intelligence in the areas of SIGINT, GEOINT and All Source intelligence domains. His thesis is focused on the disparity of technology in the government and the lack of parity with the pace of the technology development in the private sector. He may be reached at hotspur1066@gmail.com.

Disclaimer

The views expressed herein are those of the author alone.

Appendix 1

Examples of materials that can be printed with today's 3-D printers[63]

Metals

Steel
Aluminum
Titanium
Brass
Bronze
Gold
Silver
Platinum

Composites

Brass Plated with Precious Metals
Carbon Nanotubes
Inductors and Electromagnets
Polymer Transistors
Electromechanical Relays
"Artificial Muscle" Actuators
Complete Zinc Air Batteries
Elastomer strain gauges
Conductive wiring embedded in structural materials
Thermoplastic and elastomer structures and flexures

Plastics

Acrylonitrile butadiene styrene (ABS)
Acrylic
Nylon

Stone

Porcelain
Sandstone

Food

Chocolate
Sugar based candies (e.g. “gummies”)
Cake

Organics

Cartilage
Skin
Organs (e.g. Kidneys)

Notes

1 C.C Seepersad, "Challenges and Opportunities in Design for Additive Manufacturing," *3D Printing and Additive Manufacturing* 1, no. 1 (2014): 10-13.

2 D.M. Correa, C.C.Seepersad, and M.R. Haberman, "Mechanical Design of Negative Stiffness Honeycomb Materials," *Integrating Materials and Manufacturing Innovation*, 4, no. 10 (2015): 1-11.

3 C. Farivar, "Download This Gun: 3-D-Printed Semi-automatic Fires over 600 rounds - And The Department of Justice Says There's Nothing Illegal about It, Either," *Ars Technica,* March 1 2013.

4 C.C Seepersad, "Challenges and Opportunities in Design for Additive Manufacturing".

5 Geometric computer modeling is a branch of applied mathematics and computational geometry that studies methods and algorithms for the mathematical description of shapes. Three-dimensional models are central to computer-aided design and manufacturing (CAD/CAM).

6 C.M McNulty, N.Arnas, and T.A Campbell, "Toward the Printed World: Additive Manufacturing and Implications for National Security," *Defense Horizons*, DH No. 73, 2012.

7 Ibid.

8 J.Herman, "How to Get Started: 3-D Modeling and Printing," *Popular Mechanics*, March 15, 2015.

9 Stratasys Customer Support, n.d. http://www.stratasys.com/customer-support/cad-to-stl (accessed October 18, 2015).

10 R.Matulka, "How 3-D Printers Work," United States Department of Energy, June 19, 2014, http://www.energy.gov/articles/how-3d-printers-work (accessed October 9, 2015).

11 M. Molitch-Hou, "Hod Lipson, 3-D Printing, and the Fourth Industrial Revolution," *3-D Printing Industry*, April 29, 2015, http://3-Dprintingindustry.com (accessed September 26, 2015).

12 A. Knapp, "GE Engineers 3D-Printed A Working, Mini Jet Engine," *Forbes Tech*, May 11, 2015.

13 Moore's law is the observation that the number of transistors in a dense integrated circuit doubles approximately every two years. The observation is named after Gordon E. Moore, the co-founder of Intel and Fairchild Semiconductor, whose 1965 paper described a doubling every year in the number of components per integrated circuit.

14 The Internet grew at a fast pace in the 1990s as the general population discovered the power of the new medium. In July 1994, federal prosecutors won an obscenity conviction in Tennessee against the operators of a computer bulletin board system (BBS) called the Amateur Action BBS, a private porn subscription service.

15 S.Kotler, "Vice Wars: How 3-D Printing Will Revolutionize Crime," *Forbes*, July 12, 2012.

16 R.Meyer, "3-D Printed Drugs Are Here," *Atlantic Technology*, August 2015.

17 D.Basulto, "Why it Matters That the FDA Just Approved the First 3-D-Printed Drug," *The Washington Post*, August 2015.

18 D.Samadi, "You Can Now 3-D Print Prescription Drugs," Observer Innovation, August 2015.

19 Alec, "Hackers Could Exploit 3-D Printers, Stealing/Altering Designs, or Making Them Explode," *3-D Printer and 3-D Printing News*, September 2014.

20 D.Samadi, "You Can Now 3-D Print Prescription Drugs," *Observer Innovation*, August 2015.

21 M. Goodman, *Future Crimes*, (New York: Doubleday Books, 2015).

22 N.Lincoff, "3-D Drugs: Your Pharmacy Will Now Print Your Prescription," *HealthlineNew*s, August 7, 2015, http://www.healthline.com/health-news/3-d-drugs-your-pharmacy-will-print-your-prescription-080715 (accessed October 14, 2015).

23 N.Hernandez, "Is K2 Unstoppable? Synthetic Pot Confounds Regulatory Efforts," *The Austin Chronicle*, June 2015.

24 S. Kotler, "Vice Wars: How 3-D Printing Will Revolutionize Crime," *Forbes*, July 12, 2012.

25 A.Robinson, "Welcome to the Complex World of 3-D-Printed Drugs," *The Guardian Sustainable Business, Technology and Innovation,* August 21, 2015, http://www.theguardian.com/sustainable-business/2015/aug/21/welcome-to-complex-world-of-3d-printed-drugs-spritam-fda (accessed October 14, 2015).

26 K. Atherton, "3-D-Printed Gun Named After An Arrested Gunmaker," *Popular Science Technology,* May 2015. http://www.popsci.com/gun-3d-printed-tribute-arrested-gunmaker (accessed October 19, 2015).

27 C.Farivar, "Download This Gun."

28 K. Atherton, "3-D-Printed Gun Named After An Arrested Gunmaker."

29 C. Farivar, "Download This Gun".

30 Ibid.

31 The Undetectable Firearms Act prohibits the manufacture or selling of a firearm that "does not generate an [X-ray] image that accurately depicts the shape of the component." In other words, it's a federal crime to make and sell a gun that looks like something else to an airport X-ray scanner. A 3-D printer provides exactly that type of capability.

32 President Obama's gun control proposals have not, to date, been approved by Congress.

33 Intelligence, Rapid, StateMaster.com, 2015, http://www.statemaster.com/graph/gov_gun_law_pro_per-government-gun-laws-prohibited-persons (accessed October 21, 2015).

34 A comprehensive set of gun control laws are found in 27 CFR 478 - COMMERCE IN FIREARMS AND AMMUNITION.

35 A. Greenberg, "I Made an Untraceable AR-15 'Ghost-Gun' In My Office – and It Was Easy, "*Wired*, June 3, 2015, http://www.wired.com/2015/06/i-made-an-untraceable-ar-15-ghost-gun/ (accessed October 14, 2015).

36 U.S. Customs and Border Protection Stats and Summaries, April 2015.

37 National Crime Prevention Council, 2015, http://www.ncpc.org/topics/intellectual-property-theft (accessed October 15, 2015).

38 Gartner, Inc. is an American information technology research and advisory firm providing technology related insight headquartered in Stamford, Connecticut, United States.

39 The Center for Strategic and International Studies estimates that the 2014 annual worldwide loss of IP, due to all forms of theft, is 0.06% of the world's GNP, or roughly 445 billion dollars.

40 M.Halpern, "Intellectual Property Protection (3-D Printing), Gartner Hype Cycle for 3-D Printing," Gartner.com. 2015 July. http://www.gartner.com/document/3100228?ref=lib (accessed October 12, 2015).

41 "Globalization and Digitization Usher In a New Era of Intellectual Property Theft," National Crime Prevention Council, 2015, http://www.ncpc.org/topics/intellectual-property-theft/trends-globalization-and-digitalization-usher-in-a-new-era-of-intellectual-property-theft (accessed October 16, 2015).

42 Ibid.

43 Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism by Randall C. Coleman, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, Washington, D.C. , May 13, 2014.

44 K. Dempsey, and C.Paulsen, NISTIR 8023 Risk Management for Replication Devices, National Standard, Washington, D.C.: National Institute of Standards and Technology, Computer Security Division Information Technology Laboratory, 2015.

45 An example of this is the 1965 Chevrolet Stingray which introduced a new 427 cubic inch motor, but still kept the drum brakes from its smaller- engined predecessor. Successive models introduced disc brakes when owners discovered it was much more difficult to stop their more powerful Stingray.

46 The 3-D model can be secured so that it cannot be tampered with, copied, or changed, essentially acting as a form of file encryption. A digital signature can be printed into the object that can be used to identify that the object is genuine. Search engines can be used that validate that a model is a copy of a trademarked model.

47 M. Halpern, "Intellectual Property Protection (3-D Printing), Gartner Hype Cycle for 3-D Printing," Gartner.com. 2015 July. http://www.gartner.com/document/3100228?ref=lib (accessed October 12, 2015).

48 Ibid.

49 BAE Systems PLC is a British multinational defense, security and aerospace company headquartered in London in the United Kingdom and with worldwide operations.

50 Stuxnet is a 500-kilobyte computer worm that infected the software of at least 14 industrial sites in Iran, including a uranium-enrichment plant. Although a computer virus relies on an unwitting victim to install it, a worm spreads on its own, often over a computer network.

51 Alec, "Hackers Could Exploit 3-D printers, Stealing/Altering Designs, or Making Them Explode."

52 Traditional sabotage is battled by improving physical security controls as opposed to sabotage created via 3-D printing that will necessitate cyber security methods.

53 Checksums are used to ensure the integrity of a file after it has been transmitted from one storage device to another. The checksum is calculated using a hash function and is normally posted along with the download. To verify the integrity of the file, a user calculates the checksum using a checksum calculator program and then compares the two to make sure they match. Checksums are used not only to ensure a corrupt-free transmission, but also to ensure that the file has not been tampered with.

54 The list of known cyber exploits is extensive. A good reference source of significant exploits and tools to remediate them can be found at http://resources.infosecinstitute.com/the-top-five-cyber-security-vulnerabilities-in-terms-of-potential-for-catastrophic-damage/.

55 M. Halpern, "Intellectual Property Protection (3-D Printing), Gartner Hype Cycle for 3-D Printing."

56 P. Paganini, "Evolution of 3D Printing Technology Raises Security Concerns," Infotech Institute, October13, 2014, http://resources.infosecinstitute.com/evolution-3d-printing-technology-raises-security-concerns/.

57 A.C Estes, "3D-Printed Guns Are Only Getting Better, and Scarier," Gizmodo, Jan 2015, http://gizmodo.com/3d-printed-guns-are-only-getting-better-and-scarier-1677747439.

58 S.J.Clover, S. Hussain, and T. Little, "The Shape of Things to Come –The Next 18 Months in Trademarks," *World Trademark Review*, June 2013, http://www.inta.org/media/documents/wtrjune2013theshapeofthingstocome.pdf.

59 J.McLaughlin, "Regulating the Innovative World of 3-D Printing," *Law Street Technology*, May 30, 2015, http://lawstreetmedia.com/issues/technology/3d-printing-innovations-regulations/ (accessed October 13, 2015).

60 This article focused on light weapons; however, 3-D printers will have the capability of manufacturing larger and more devastating weapons in the near future. Manufacture of shaped charges using C4 disguised as almost any object will soon be possible. As 3-D printers become more capable, more complex weapons will be able to be manufactured such as deadly chemical weapons.

61 P.J.Cook, S.T.Parker, and H.A.Pollack, "Sources of Guns to Dangerous People: What We Learn by Asking Them," *Preventive Medicine*, 79 (April 2015): 28-36.

62 J.McLaughlin, "Regulating the Innovative World of 3-D Printing."

63 Shapeways 3D Printer Materials, n.d. http://www.shapeways.com/materials (accessed October 12, 2015).