

# 3D Printing: The Future Crime of the Present

Justin D. Fruehauf  
fruehaufj@rmu.edu  
Computer and Information Systems

Francis X. Hartle  
hartle@rmu.edu  
Social Sciences

Fahad Al-Khalifa  
faast100@mail.rmu.edu

Computer and Information Systems  
Robert Morris University  
Moon Township, PA 15108, USA

## Abstract

In his 2015 book *Future Crimes* Marc Goodman discusses the impact of emerging technologies on society arguing that these technologies test the very fabric of the current nation state centered world (Goodman, 2015). Goodman states that thanks to the technologies developed in the late 20th and early 21st century the Westphalian system that controlled national borders since 1648 is rapidly becoming irrelevant and archaic (Goodman, 2015). None of the technologies hold the potential impact as that of 3 dimensional (3D) printing technology. First and foremost, 3D printing technology is not a future technology that will be used by criminals; it is already happening. 3D printing is not just a physical technology, 3D printing represents a bridge between physical engineering (and thus physical crime) and cyber-crimes. The purpose of this paper is to provide a brief overview of 3D printing technologies and the threats it poses as a cyber security issue.

**Keywords:** 3D Printing, Cyber Crime, Cyber Security, intellectual property

## 1. INTRODUCTION

In his 2015 book *Future Crimes* Marc Goodman discusses the impact of emerging technologies on society. More to the point, he argues that these technologies test the very fabric of the current nation state centered world (Goodman, 2015). Thanks to the digital web-accessible technologies developed in the late 20th and early 21st century, Goodman believes the Westphalian system that controlled national borders since 1648 is rapidly becoming irrelevant and archaic (Goodman, 2015).

Criminals are quick to seize upon new technologies in order to gain a strategic advantage over law enforcement agencies worldwide (Goodman, 2015; Silbergliitt, Chow, Hollywood, Woods, Zaydman, & Jackson. 2015). In some instances, authorities are able to keep pace with the high tech criminal actors, but this is typically not the case. Compounding the problem is the geographic freedom of the Internet. Crimes can be committed from across borders. Because rules are often non-existent, contradicting, or differ between nations a crime in one sovereign state may be legal elsewhere,

leaving the question of jurisdiction unanswered (Subramanian, & Sedita, 2015).

While many of the technologies discussed in Future Crimes offer a disturbing look into potential criminal activity, none hold the immensely ominous impact as that of 3 dimensional (3D) printing technology. First and foremost, 3D printing technology is not a future technology to be used by criminals; it is already happening. As this paper will discuss, 3D printing technology, which has existed since the 1980s as a primitive prototyping tool, is already proving to be a criminal tool. The technology is only now beginning to find traction due to the rise of other technologies such as faster Internet connections, digital cameras, and miniaturization (Goodman, 2015).

3D printing is not just a physical technology, 3D printing represents a bridge between physical engineering (and thus physical crime) and cyber-crimes. Digital files developed or stolen in one country can be transported around the world via the Internet to be physically created. In many instances, the laws governing any of these countries are too primitive to cover this type of cyber-crime (Silberglitt et al 2015). The purpose of this paper is to assess the current state of 3D printing technologies and the threats it poses as a cyber security issue. It is the hope that by highlighting these issues, a serious discussion will ensue regarding the role information security specialists and law enforcement play in addressing the current and potential risks posed in this paper.

A review of the literature shows that as of 2016 little is written regarding the 3D printing as a cyber security threat. As such much of the information in this article was culled from both peer reviewed research and news articles and other online mainstream media outlets. It is presented below as a series of brief case studies addressing the following research question:

Research Question: How is 3D printing technology changing the manner in which cyber security and cyber-crimes must be addressed?

## 2. 3D PRINTING

3D printing or additive manufacturing (AM) is a process of making a three dimensional solid objects from a scanned preexisting prototype or creating a computer aided design (CAD) digital file. The 3D printing process begins with the creation of a CAD, or digitally generated virtual

design of an object. The CAD can be generated in one of two ways; manually through the use of a 3-dimensional modeling program or by scanning an existing real-world object with a 3D scanner. The 3D scanner then generates a virtual model of the object. (Campbell, Williams, Ivanova, & Garrett, 2011; 3Dprinting.com)

Additive manufacturing creates an object by laying down successive layers of material forming the desired object rather than deductive manufacturing that is common today, (Campbell et.al, 2011; 3Dprinting.com). While all 3D printers use additive methods there are several manners in which the process is conducted. These include fused deposition modeling (FDM) that utilizing plastics and metals that are melted and layered to harden when excreted; stereolithography (SLA) printers that use light to solidify liquid resin when exposed to a specific light wavelength; selective laser sintering (SLS) printers that use high energy laser to solidify a powder medium into various metals and plastics; laminated object manufacturing (LOM) that cuts and glues multiple materials into a specific object. (Griffey, 2014). In addition, multi-material 3d printers have been developed to construct complex, electronic products (Sitthi-Amorn, Ramos, Wangy, Kwan, Lan, Wang, & Matusik, 2015).

Though the technology has existed since the 1980s as a means of creating prototypes, 3D printing technology is emerging as a production level technology at least since 2014 (Gartner, 2014). For more traditional manufacturing, 3D printing technology is already becoming the de facto means of production for many retail products. The Gartner report claims that "3D printer shipments will more than double every year between 2015 and 2018" (Gartner, 2014).

## 3. INTELLECTUAL PROPERTY THEFT

The impact of the use of this technology on intellectual property rights is potentially crippling. As 3D printing technology becomes affordable (personal 3D printers can be purchased for approximately \$500 US (Gartner, 2014)) the ability of people to pass electronic files anywhere in the world via the Internet and produce an object at home has staggering implications. Global predictions of losses over \$100 billion by 2018 annually due to intellectual property theft and the use of 3D printing technology (Gartner, 2014).

## **The United States: A Case Study of intellectual property theft involving 3D printing**

### **United States Tariff Act of 1930**

Rooted in the 1922 Fordney-McCumber Act, the US Congress enacted the United States Tariff Act of 1930 (also known as the Smoot-Hawley Tariff Act) to protect domestic industries from foreign competition. The tariff raised duties on imports by 20%. It was originally crafted to combat dropping prices on agricultural products brought on by the rise in European agriculture due to the recovery from World War I (Beaudreau, B, 2016). Often cited as a cause of The Great Depression and the rise of isolationism, the Smoot-Hawley Tariff Act remained a part of US policy, continuing to evolve over the subsequent decades with major amendments coming in 1974 and 1988 (Aranoff, 2010).

### **Section 337**

From a technology perspective the most critical part of Smoot-Hawley is what is commonly known as Section 337. Section 337 makes it illegal to infringe on specified intellectual property rights and other "unfair competition in import trade". According to the United States International Trade Commission (USITC), the United States government body that investigates 337 cases, the majority of 337 investigations revolve around patent or trademark infringements (USITC, Pg 1, 2009). Key among the 1974 and 1988 amendments was the expansion of the role of the USITC to seek to enforce the statutes of the tariff, particularly those claims involving Section 337 (Aranoff, 2010). The ITC defines trademarks and patents as the following:

- Trademarks are word(s), symbol(s) or any combination thereof used to designate a product or company, giving it uniqueness (United States Patent and Trade Office (USPTO)).
- A patent is a property right for an invention (USPTO). There are three types of patents;
  - o Utility patents - Granted for inventing, discovering, or improving upon a process, machine, article of manufacture, or composition of matter (USPTO)
  - o Design patents - Granted for inventing a new, original, and ornamental design for an article of manufacture (USPTO)
  - o Plant patents - Granted for discovering or creating and successfully reproducing a new type of plant (USPTO)

In fact, most patents are held on physical objects (Thimmesch, 2015). Their litigation through 337 investigations run a "traditional" path through the judiciary system in the US.

### **Align versus ClearCorrect: 337 meets 3D Printing**

In 2012 Align Technology, headquartered in California, filed a lawsuit against Texas-based ClearCorrect alleging that ClearCorrect violated Section 337. Align's argument focused on the use of 3D printing and the process of using electronic files to make medical devices for patients (Thimmesch, 2015). Align maintains a patent for its process of using scanned digital files and 3D printers to create its product. Its suit alleges that ClearCorrect violated this patent (Thimmesch, 2015).

### **The Case**

Align offers a product line of plastic teeth aligners, known as Invisalign, which are generated through the use digital scans of patient's teeth (Thimmesch, 2015). These scans are then used to create electronic 3 Dimensional models of teeth aligners made to perfectly fit the patient's mouth. The 3D models are used as guides for producing the actual aligners through 3D printers—Align applied for and was granted a patent for this process in 2001 (Thimmesch, 2015).

ClearCorrect, a Texas-based company, used a similar process to produce similar teeth fittings (Thimmesch, 2015). However, ClearCorrect would send the electronic scans to ClearCorrect Pakistan, a company located in Lahore Pakistan (Thimmesch, 2015). ClearCorrect Pakistan was tasked with generating 3D models from the scans that were then sent back to the Texas-based ClearCorrect facility to 3D printers for physical part production (Thimmesch, 2015).

It was this electronic transmission of digital files from Texas to Pakistan and back to Texas that formed the bases for the 2012 Section 337 Complaint filed by Align against ClearCorrect (Thimmesch, 2015). Citing their patent on the method for generating mouth molds, representatives from Align argued that the process used by ClearCorrect violated Section 337 because the transmission of the files qualified as an "importation of articles" from a foreign country. As such ClearCorrect was implementing an unfair practice in the United States (Thimmesch, 2015).

### **The Ruling and the Appeal**

In April of 2014 the International Trade Commission ruled in favor of Align, arguing that the principle of Section 337, the importation of articles, also includes the transmission of digital data. Furthermore, the digital data, the Commission maintained, were the true articles of import and commerce (Osborn, 2014).

The issuing of this ruling caused legal experts to re-examine past patents and how they advised their clients. Lucas Osborn, director of the Intellectual Property Law Program at the Campbell School of Law, cited two major issues from the Align versus ClearCorrect case.

1. How should patent law treat claims directed to digital representations of physical objects?
2. How should patent law treat claims directed only to physical articles where the alleged infringement involves only or primarily digital renderings of the physical articles?

(Osborn, 2014)

Osborn notes that the details of this case show that Align's patents are directed to the first issue. As such those looking to protect their physical products should also patent their digital versions (Osborn, 2014). The second issue, he argues, presents the dilemma facing companies. As most patents were issued for physical objects, divining court rulings on electronic representations of physical objects is unclear. Osborn maintains that this is similar to the digital media legal issues faced by film and music companies. Companies must move to protect digital images of their products as well or risk massive revenue losses (Osborn, 2014).

In June 2015 the United States Patent and Trademark Office (USPTO) granted ClearCorrect's request to reexamine the US patents held by Align (Seiders, 2015). The USPTO stated that it will issue a formal rejection of some of the patents as un-patentable due to its revolving around "core concepts of orthodontic treatment" existing for decades basing this on prior art submitted by Align for the patent (as seen in the Align patent drawing to the right) (Seiders, 2015). The matter is now being heard by a US Federal Appeals Court.

Companies scramble to patent electronic copies of their physical products because current patent laws do not protect them. Still unclear is how changes to digital designs will be viewed by US courts. As Josh Greenbaum of Enterprise

Application Consulting notes "IP protection has always lagged technological advances, and 3D printing isn't any different: while it is clearly illegal to print a patented object, merely possessing the plans for printing that object does not violate patent law" (Wired, 2015).

Furthermore, even if US law protect companies, this is only in the United States. Once digital designs are exposed to the Internet they are easily pirated for production in countries that have no patent laws. While this is not a new issue for manufacturers it has only existed in the physical world, this is no longer the case. Foreign entities can easily produce digital designs. The conflicting rules and regulations among US government entities in this case, coupled with the growing complexities of globalized industry demonstrates that government regulations must be re-examined and modified to fall in line with the impact of 3D printing technology.

### **4. WEAPONS PRODUCTION**

In May of 2014 Andy Greenberg, writing for [www.wired.com](http://www.wired.com) reported on the advancements in 3D printed firearms made almost entirely of plastic and printed by private home users (2014). "It took only weeks for digital gunsmiths to improve upon the first fully 3-D printed gun. Defense Distributed printed the first Liberator in May, 2013, using a second-hand refrigerator-sized Stratasys 3-D printer it bought for \$8,000. Later that month, a gun enthusiast in Wisconsin riffed on the Liberator to produce a working firearm for far less, using a \$1,725 Lulzbot printer with less than \$25 in plastic. It fired eight .38-caliber bullets without damage" (Greenberg, 2014).

Later than year Greenberg reported that a non-profit group designed a computer-controlled (CNC) milling machine for under \$1200 designed to make aluminum weapon parts. While CNC is reductive manufacturing, like 3D printing, the software and programming that it used is easy to share and use. This technology coupled with 3D printing could allow individuals to manufacture entire weapons systems (Greenberg, 2014 Oct).

Greenberg goes on to state that US legislators have done little to curb the creation of 3D printed weapons. The US Congress has yet to pass an amendment to the Undetectable Firearms Act banning the creation of 3D printed firearms (Greenberg 2014). In fact it is currently legal under United States 18 U.S. Code Chapter 44 – Firearms for anyone in the United States to

produce their own 3d printed firearm provided they create it for home defense use (Gilger-VanderZanden).

Firearms have always been produced by gun enthusiasts. In fact, there is a cottage industry for gunsmiths who make their own weapons. The milling of metal and wood to produce weapons as well as the availability of trigger mechanisms and other parts via the internet is common practice (Jacobs, & Haberman, 2016).

The concerns of the US government regarding home manufactured firearms are many. One, they can't track purchases. More complex firearms like the AR-15 and AK 47 require the purchase of parts with serial numbers. One could legally mill a part without a serial number but could not sell it. CNC and 3D printing of complex parts would automate the production of controlled parts. In addition, the CNC and 3D equipment used to produce the weapons is expensive. A typical weapon is many times more expensive than the equipment to produce a single firearm. Perhaps this low ROI could be used as motivation to manufacture and sell illegal untraceable guns. Second, the government may not want the transfer of weapons (firearm) manufacturing data to fall into the wrong hands (Jacobs, & Haberman, 2016). Although this is a legitimate argument it seems far-fetched that nations would rely on this non-traditional, slow process of firearms production. Although CNC and 3D printer manufacturers and programmers can "legally" make weapons and weapon parts, they are prohibited from making them widely available on the internet based on arms control legislation. Lastly, the federal and state governments have a legitimate concern in keeping firearms out of the hands of the mentally ill and/or persons' intent on mass killings. The idea of producing assault style weapons that hold high capacity magazines could be tantalizing for terrorist or their inspired followers. A slew of government checks and tripwires could be evaded using the technology (Jacobs, & Haberman, 2016). This combination of internet technologies and software to produce weapon designs and the use of the 3D printers to produce these weapons creates a cyber trafficking dilemma not easily overcome by law enforcement agencies bound by current laws and civilian rights.

A more immediate and legitimate concern for the nefarious use of 3D printers is the manufacture of layered explosives and complex parts for bombs including nuclear components. Printers that combine chemical, metal and plastics could,

someday, produce assembled explosive weapons at the push of a button (Kroenig, & Volpe, 2015).

## 5. THE CHEMPUTER

In July 2012 Professor Lee Cronin of Glasgow University announced that he turned a 3D printer into a "universal chemistry set" or "chemputer" capable of producing prescription drugs using downloadable chemistry instructions (<http://www.kurzweilai.net>). Cronin stated that nearly all drugs are made of carbon, hydrogen and oxygen, as well as readily available agents such as vegetable oils and paraffin (<http://www.kurzweilai.net>). "With a printer it should be possible that with a relatively small number of inks you can make any organic molecule" (<http://www.kurzweilai.net>).

As Steve Kotler, a contributing reporter for Forbes.com, discusses, it will not take long for the "chemputer" to be hacked and used to make illicit drugs (Kotler, 2012). Certainly there are laws in every country regarding what drugs are legal, but how to enforce these laws when the formula for the drugs can be obtained on the globally accessible World Wide Web and made in private will be almost impossible. It would require a total policing of the entire Internet. Formulas for drugs could simply be embedded or coded in files passed between illegal drug producers.

Once a formula is available, there would be no way to remove it completely from the Internet. There simply are no laws to prevent this from occurring, the only recourse law enforcement agencies have is to catch "home chemists" in the act. The chemputer has not been made readily available to the public, however this does not mean that it is not currently being used by narcotic producers, there simply is no way to know for sure.

## 6. BANK FRAUD

3D printing is already being used in conjunction with traditional ATM skimming. In 2014 Todd Halterman of 3Dprinterworld.com reported that "Bulgarian and Spanish authorities, working alongside agents of Europol's European Cybercrime Centre in The Hague" uncovered and a Bulgarian organized crime network using 3D printers to commit varying crimes such as "ATM skimming, electronic payment fraud and document forgery" (Halterman, 2014). The report states "the thieves used 3D printing equipment to make convincing, but fake, plastic card slot bezels they installed on ATM machines

and Point of Sale terminals" (Halterman, 2014). The extent of stolen user information ranged from banking terminals in Italy, France, Spain, Germany, and Turkey (Halterman, 2014). The user information helped create fake payment cards used to make cash withdraws in countries such as the Philippines and Peru (Halterman, 2014).

## 7. CONCLUSIONS

3D printing is a technology already impacting the criminal world, in some ways we are aware of, but more likely many that have yet to be discovered by law enforcement officials. 3D printing technology is often cited as the future for global manufacturing (Federico-O'Murchu, 2014). Its lower production costs due to the additive process, the ability to digitally transmit CADs to local production facilities thus reducing shipping costs, and the dropping cost of the technology itself all offer immense benefits. Factor in the universal nature of the technology and the myriad materials from plastic to organics such as pharmaceuticals make and 3D printers are truly beneficial to human society (Federico-O'Murchu, 2014). Imagine a doctor in remote Africa being able to produce life-saving medicines such as anti-venoms with just the click of a mouse button.

Yet as the above examples demonstrate the technology is already being used for criminal endeavors and will only continue to grow in this capacity. While the use of 3D printing technology by bank thieves in Europe is concerning, is somehow refreshing for its traditional crime approach, it's still simply pick-pocketing. Far more disturbing is the idea of extremists combining the readily available firearms CADs and chemputer concepts to produce chemical and biochemical devices with only one intent. 3D printing is not a future crime technology, it is a past technology finding new life because of scanning technology and the World Wide Web.

## 8. REFERENCES

- Aranoff, S. (2010, May). "The U.S. International Trade Commission, Section 337, and patents – Looking back and looking forward". The ITC Comes to Silicon Valley. Retrieved from <https://www.law.berkeley.edu/files/Aranoff-ITC-Comments.pdf>
- Beaudreau, B. C. (2016). The petition against the Smoot-Hawley Tariff Bill: what 1,028 economists overlooked. *real-world economics review*, 124.
- Federico-O'Murchu, L. (2014, May). How 3-D printing will radically change the world. Retrieved from <http://www.cnbc.com/2014/05/09/will-3-d-technology-radically-change-the-world.html>
- Jacobs, J., & Haberman, A. (2016). 3D Printed Firearms, Do-It-Yourself Guns & The Second Amendment. *Law and Contemporary Problems*, Forthcoming, 16-27.
- Jason, G. (2014). The Types of 3-D Printing. *Library Technology Reports* [serial online]. July 2014;50(5):8-12. Available from: Education Research Complete, Ipswich, MA.
- Gilger-VanderZanden, J. (2016). Are 3D guns legal? <http://www.criminaldefenselawyer.com/resources/are-3d-guns-legal.htm>
- Goodman, M. (2015). *Future Crimes*. Doubleday.
- Greenbaum, J. (2012, March). Illegal, immoral, and here to stay: counterfeiting and the 3D printing revolution. Retrieved from <http://www.wired.com/insights/2015/02/illegal-immoral-and-here-to-stay-counterfeiting-and-the-3D-printing-revolution/>
- Greenberg, A. (2014, May). How 3-D Printed Guns Evolved Into Serious Weapons in Just One Year. Retrieved from <http://www.wired.com/2014/05/3d-printed-guns/>
- Greenberg, A. (2014, Oct). That \$1,200 Machine for Making Untraceable Guns Just Sold Out in 36 Hours. Retrieved September 04, 2016, from <https://www.wired.com/2014/10/1200-machine-making-untraceable-guns-just-sold-36-hours/>
- Halterman T. (2014, October). How 3D Printing Has Already Revolutionized Crime. Retrieved from <http://www.3dprinterworld.com/article/how-3d-printing-has-already-revolutionized-crime>
- Kroenig, M., & Volpe, T. (2015). 3-D printing the bomb? The nuclear nonproliferation challenge. *The Washington Quarterly*, 38(3), 7-19.
- Kotler, S. (2012, July). Vice Wars: How 3-D Printing Will Revolutionize Crime. Retrieved from <http://www.forbes.com/sites/stevenkotler/2012/07/31/the-democratization-of-vice-the-impact-of-exponential-technology-on-illicit-trades-and-organized-crime/>

- Osborn, L. (2014, April). Digital patent infringement and the ITC. Patentlyo. Retrieved from <http://patentlyo.com/patent/2014/04/digital-patent-infringement.html>
- Seiders, A. (2015, June). U.S. Patent Office sides with ClearCorrect to reexamine Invisalign patent portfolio. Retrieved from <http://blogclearcorrect.com/category/legal.aspx>
- Silberglitt, R., Chow, B. G., Hollywood, J. S., Woods, D., Zaydman, M., & Jackson, B. A. (2015). Visions of Law Enforcement Technology in the Period 2024-2034. Rand Corporation.
- Sitthi-Amorn, P., Ramos, J. E., Wangy, Y., Kwan, J., Lan, J., Wang, W., & Matusik, W. (2015). MultiFab: a machine vision assisted platform for multi-material 3D printing. *ACM Transactions on Graphics (TOG)*, 34(4), 129.
- Subramanian, R., & Sedita, S. (2015). Are Cybercrime Laws Keeping up with the Triple Convergence of Information, Innovation and Technology?. *Communications of the IIMA*, 6(1), 4.
- Thimmesch, D. (2015, January). 3D printing at the center of controversial intellectual property debate. Retrieved from <http://3Dprint.com/34255/itc-intellectual-property/>
- Encyclopedia Britannica Editors. (2015). Smoot-Hawley Tariff Act. Retrieved from <http://www.britannica.com/topic/Smoot-Hawley-Tariff-Act>
- Gartner Group. (2014, October). Gartner says worldwide shipments of 3d printers to reach more than 217,000 in 2015. Retrieved from <http://www.gartner.com/newsroom/id/2658315>
- United States International Trade Commission.(USITC) (2009, March). Section 337 investigations: Answers to frequently asked questions. United States International Trade Commission.
- United States Patent and Trademark Office (USPTO). Trademark basics. Retrieved from <http://www.uspto.gov/trademarks-getting->
- [www.3Dprinting.com](http://www.3Dprinting.com) (2015). Retrieved from <http://3Dprinting.com/what-is-3D-printing/>
- [www.kurzweilai.net](http://www.kurzweilai.net). (2012, June). Retrieved from [http://www.kurzweilai.net/the-chemputer-that-could-print-out-any-drug?utm\\_source=KurzweilAI+Weekly+New+sletter&utm\\_campaign=b60382892c-UA-946742-1&utm\\_medium=email](http://www.kurzweilai.net/the-chemputer-that-could-print-out-any-drug?utm_source=KurzweilAI+Weekly+New+sletter&utm_campaign=b60382892c-UA-946742-1&utm_medium=email)

