Liability Exposure when 3D-Printed Parts Fall from the Sky

Lynne Graves, Mark Yampolskiy, Wayne King, Sofia Belikovetsky, Yuval Elovici

Chapter 3

LIABILITY EXPOSURE WHEN 3D-PRINTED PARTS FALL FROM THE SKY

Lynne Graves, Mark Yampolskiy, Wayne King, Sofia Belikovetsky and Yuval Elovici

Abstract Additive manufacturing, also referred to as 3D printing, has become viable for manufacturing functional parts. For example, the U.S. Federal Aviation Administration recently approved General Electric jet engine fuel nozzles that are produced by additive manufacturing. Because additive manufacturing is integrated with cyber technology, a number of security concerns have been raised. This chapter specifically considers attacks that deliberately sabotage the mechanical properties of functional parts produced by additive manufacturing; the feasibility of these attacks has already been discussed in the literature.

Investments in security measures directly depend on cost-benefit analyses conducted by the participants involved in additive manufacturing processes. This chapter discusses the entities that can be considered to be financially liable in the event of a successful sabotage attack. The analysis employs a model that distinguishes between the levels at which the additive manufacturing process has been sabotaged. Specifically, it differentiates between the additive manufacturing service provider and the various commodity suppliers. For each possible combination of injured party and level of attack, the involved parties that may face liability exposure are identified. This is accomplished by analyzing the necessary components that establish liability. The analysis reveals that liability potential exists at all levels of the additive manufacturing process in the event of a sabotage attack. For this reason, it is imperative that the involved actors conduct or re-evaluate their cost-benefit analyses and invest in security measures.

Keywords: Additive manufacturing security, sabotage, liability

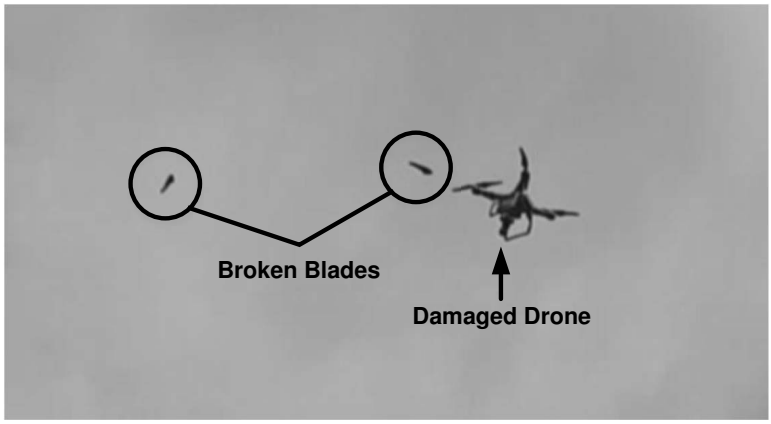

Figure 1. Failure of a sabotaged propeller in the `dr0wned` study [4].

1. Introduction

In 1947, a science fiction author envisioned 3D-printed spaceships [33]. Since then, reality has converged with vision. Additive manufacturing (AM) technology, also referred to as 3D printing, is now viable for industrial manufacturing, including the creation of functional parts for safety-critical systems. A recent example is General Electric's use of additive manufacturing to create fuel injection nozzles for the next generation LEAP jet engines [16] – a commitment of $22 billion to date [8, 20]. Meanwhile, the worldwide annual industry revenue from additive manufacturing is increasing rapidly and is expected to exceed $21 billion by 2020 [8].

The American Society for Testing and Materials (ASTM) defines seven additive manufacturing process categories [2, 46]. The shared characteristics are that they use a highly computerized process and that a 3D object is produced based on a digital model representation by depositing and fusing thin layers of source material.

Due to its reliance on computerization, additive manufacturing is susceptible to a variety of attacks. These include sabotage attacks, which deliberately degrade the mechanical properties of manufactured parts [4, 31, 51]. The `dr0wned` study [4] demonstrates the danger of sabotage attacks on functional parts. In the study, researchers compromised a benign 3D printing environment, and accessed and modified the design file of the replacement propeller of a quadcopter drone in a manner that was unique to additive manufacturing. The compromise caused the propeller to break in flight. The image in Figure 1 is taken from the video recording of the experiment. It shows the broken propeller blades and the drone falling from the sky.

Similar attacks on functional parts for safety-critical systems could result in injury and loss of life. These incidents would lead to time-consuming investigations, expensive liability litigation and reputation loss for the involved

companies as well as negative public perceptions of the additive manufacturing industry. This chapter examines the various layers and avenues of liability exposure incurred by sabotage attacks on additive manufacturing.

2. Related Work

This section discusses research on additive manufacturing security and issues related to additive manufacturing liability exposure.

2.1 Additive Manufacturing Security

At the end of 2017, approximately seventy papers had been published on additive manufacturing security [47]. This section only considers research related to sabotage attacks.

Yampolskiy et al. [48] have studied the similarities and differences in security issues for additive and subtractive manufacturing (also referred to as computer numerical control (CNC) manufacturing). In their comparison, Yampolskiy and colleagues identified significant areas of overlap, including classical cyber security. However, they also identified significant and fundamental differences, including variations in possible manipulations and achievable effects.

Sturm et al. [32] have raised the possibility of attacks on large metal-alloy parts (e.g., used in jet turbines) that could cause operational failures. They identified four items that were vulnerable to attack: (i) computer-aided design (CAD) model; (ii) stereolithography (STL) file; (iii) toolpath file; and (iv) physical machine. Sturm and colleagues focused on STL files, and discussed scenarios involving corruption, scaling, indentation/protrusion, vertex movement and void attacks. They concluded that the most dangerous attacks would target structurally-strategic locations while being small enough to evade detection. They also highlighted an almost 50% decrease in failure strain for defective specimens and the inability to detect defects through mass, weight and visual inspections.

Zeltmann et al. [51] also studied similar attacks. They employed two different materials in order to embed defects. They found that the defects were undetectable with ultrasonic scans and that the defects deformed instead of cracking under stress. They also empirically investigated the impact of maliciously adjusting the printed object's orientation, an attack previously proposed by Yampolskiy et al. [49], and concluded that a 45° orientation reduced failure strain.

In their study of additive manufacturing using metals and alloys, Yampolskiy et al. [49] identified sabotage attacks that could be perpetrated by manipulating manufacturing process parameters. In the case of additive manufacturing using powder bed fusion, the alterable parameters include the scanning strategy, heat source energy and layer thickness. Another attack involves the compromise of the source material supply chain, where the source powder is substituted or mixed with a powder of different size or chemical composition, resulting in performance degradation of the manufactured parts.

Pope and Yampolskiy [26] have observed that timing disturbances in network communications (e.g., packets coming too late, too early or out of order) may impact industrial-grade additive manufacturing equipment and, by extension, the quality of the manufactured parts. Other factors include power interruptions or fluctuations to the manufacturing equipment.

Moore et al. [22] demonstrated printer firmware modification attacks. Their malicious firmware was able to substitute entire part models as well as perform less obvious modifications such as changing the extrusion rate. In earlier work, Moore et al. [21] examined the vulnerabilities of open-source software used with desktop 3D printers. They employed static source code analysis, dynamic USB communications analysis and architectural analysis to identify a number of security weaknesses.

Malicious code was key to an attack demonstrated by Belikovetsky et al. [4]. To demonstrate a complete attack chain, Belikovetsky and colleagues created a scenario in which an Internet-connected computer that controlled 3D printing was infected by malware delivered via email. The malware modified the STL file to introduce defects that would accelerate material fatigue. The modification resulted in propeller failure during flight, leading to the complete destruction of the drone and payload. A key concern brought about by the scenario is that the sabotaged propeller passed visual, weight and initial operational inspections.

2.2 Liability Exposure

Under current products liability law, parties can be held strictly liable for defective products. The concept is based on fairness, societal loss distribution and public safety [43]. To be held liable, the party must be commercially engaged in selling, must sell or distribute a product and the product must be defective [43]. Additionally, the product is expected to reach the end user without substantial change [11].

Engstrom [11] examined the liability of defective home-printed products, and identified the possible defendants as the hobbyist/inventor, digital designer and printer manufacturer. However, she argued that they are unlikely to be held liable because the hobbyist/inventor fail the commercial standard and the designer fails the product standard because code has been held not to be a product and, even if it were to change, the design code is modified significantly during the 3D printing process; for the printer manufacturer to be held liable, the printer had to be defective when it left the manufacturer's possession.

Liability can be primary or secondary. Reddy [27] discussed both types of liability when explaining the ramifications of 3D printing for intellectual property, contraband and at-home regulated item production. Primary liability evolves from the act while secondary liability can result from financial benefit and supervision or knowledge of and contribution to the act. Reddy concluded that regulations are required to address all levels of liability in additive manufacturing.

Strict liability is not the only cause of action that can be applied to 3D printers. Berkowitz [5] has analyzed the applicability of negligence and breach

of warranty as well as strict liability and the related defenses. She proposed retaining strict liability for 3D printing, but creating a new affirmative defense for micro-sellers to meet the social policies of balancing protection with fairness.

Comerford and Belt [9] have also discussed strict liability, negligence and breach of warranty when they examined the exposure of scanning service providers and large-scale manufacturers. They suggested that, with definitive roles and responsibilities, the entire additive manufacturing chain can be characterized by the authorized dealer distribution chain construct, albeit virtual in nature. They also contended that contracts and insurance provide protection and indemnification in case of liability.

Supply chain categorization forms the basis of the liability analysis of Nielson [23]. Nielson examined liability in four product delivery frameworks, finding that the causes of action are difficult to pursue under all the frameworks, but more likely against a non-manufacturing seller.

Malloy [19] has proposed several avenues of recovery based on analyses of three actors: (i) printer manufacturer; (ii) computer-aided-design file creator; and (iii) object printer. He analyzed each actor with regard to design manufacturing and warnings of instruction defects, and provides strict liability grounds for each actor.

Wang [45] examined 3D printing services as a liability target. He discussed the use of risk-utility analysis to determine design defects. The analysis combines risk, utility and consumer expectations. Risk considers inherent safety and mitigability, and utility encompasses reasonable alternatives. Wang concluded that the impact of wrong materials can provide a defense to actors other than the supplier.

3. Attack Scenario

This section describes a typical additive manufacturing workflow and presents a sabotage attack scenario that targets the workflow.

3.1 Additive Manufacturing Workflow

Additive manufacturing can be used as an integral part of a manufacturer's process or it can be outsourced to external companies that provide additive manufacturing as a service. Figure 2 presents a typical additive manufacturing workflow that emphasizes the cyber and physical interactions between the various actors.

The additive manufacturing service provider infrastructure includes additive manufacturing machines, various post-processing equipment (e.g., hot isostatic pressing (HIP) equipment), non-destructive testing equipment (e.g., computer tomography system) and an information technology (IT) infrastructure. These infrastructure components are typically provided by different vendors that are often also responsible for equipment maintenance. Maintenance typically includes hardware maintenance, software and firmware updates, and equipment calibration.

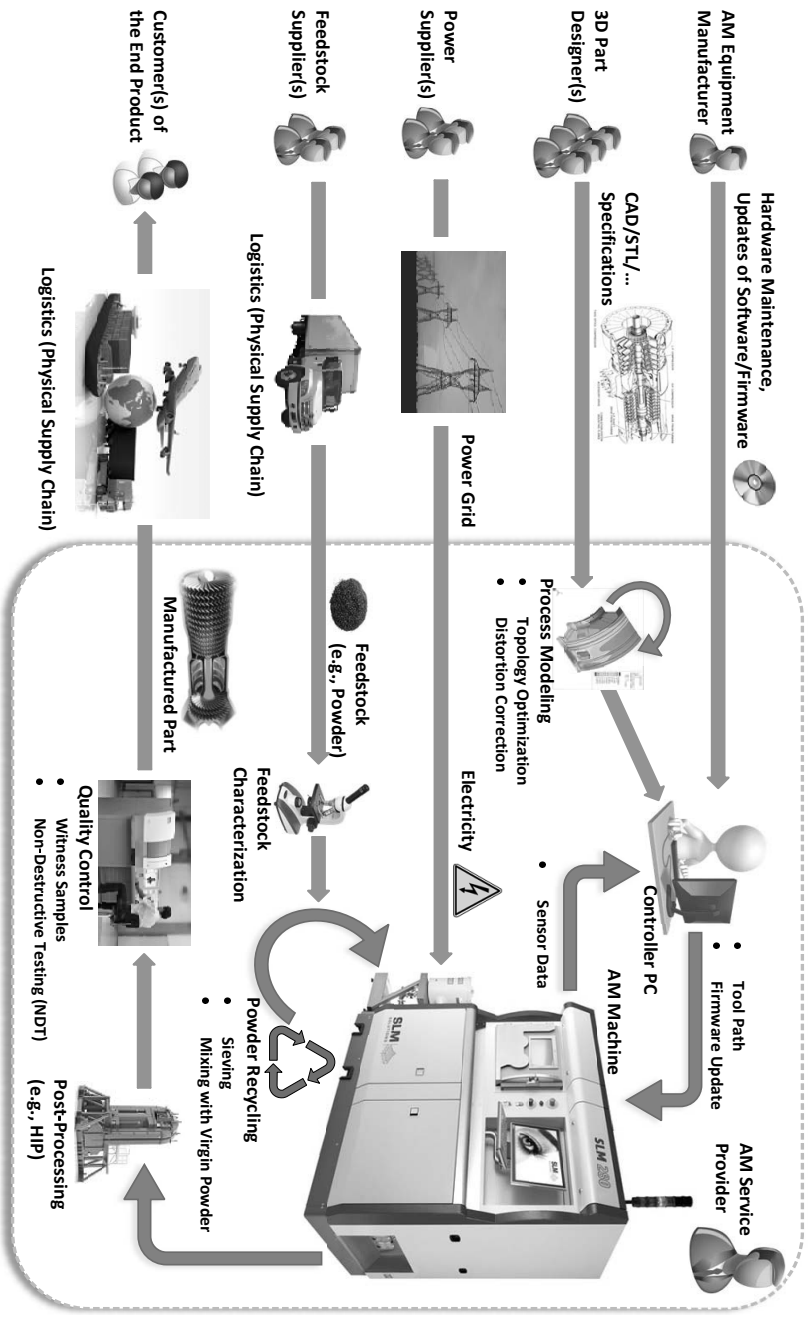

Figure 2. Additive manufacturing workflow [47].

The additive manufacturing service provider relies on digital model files (typically in the STL, AMP and 3MF file formats) and physical commodities like feedstock (i.e., source materials) and power. Depending on the expertise and scope of the manufacturer, the 3D part designer may be independent of the service provider or function as an internal entity, The physical commodities are commonly provided by external suppliers.

The physical commodities may also be involved in complex on-site processes. For example, feedstock can be characterized based on its quality. However, this is a time-consuming and expensive task. Therefore, additive manufacturing service providers often rely on characterizations provided by their suppliers. Additionally, to reduce costs and negative environmental impact, additive manufacturing processes such as powder bed fusion reclaim the unused powder, which is subsequently re-processed and reused.

The information technology infrastructure of a service provider includes computers, networks and software. In an industrial setting, software is used to optimally orient a part for a build, add support structures, lay out the build plate and slice the build into the desired layers. Process simulation software can be used to reduce geometric distortions arising from residual stress. A controller computer is used to translate a design file to equipment-specific toolpath commands that specify the 3D object to be manufactured. The toolpath commands are sent for execution to a 3D printer via a computer network. Due to the integration of *in situ* quality diagnostics in additive manufacturing machines, sensor information is commonly fed back to the controller computer via the network.

Quality assurance (QA) activities on a manufactured part may include nondestructive testing such as computer tomography and ultrasonic testing. However, while these testing methods are well-suited to subtractive manufacturing, no single technique is applicable to all types of additively-manufactured parts [1, 12, 46].

3.2 Sabotage Attack

The `dr0wned` study of Belikovetsky et al. [4] demonstrated the feasibility of sabotage attacks. Their study implemented the entire chain of a sabotage attack. They obtained backdoor access to the controller computer using a classical spear-phishing attack over an external network connection. Next, they searched the compromised computer for STL files. After locating the drone propeller STL file, they downloaded the file. Following this, they analyzed the file to determine the modifications that would accelerate fatigue; specifically, fatigue that would cause the propeller to break after a certain amount of normal operation. After they verified that the modified propeller would reliably break within three minutes, they utilized the same backdoor to replace the original STL file with the corrupt version. Subsequently, the corrupted file was used to print a replacement propeller for the quadcopter drone. During the flight test, the propeller broke in normal flight within the anticipated time frame. The

drone suffered catastrophic failure and plummeted to the ground, resulting in the destruction of the drone and its payload.

The `dr0wned` scenario is a viable threat to the manufacturing industry. This assessment is supported by the fact that Belikovetsky and colleagues incorporated attack concepts that had been demonstrated in industrial settings, including a spear-phishing attack, which established a backdoor to support the exfiltration, infiltration and corruption of files. The uniqueness of the threat originates from the effects that the modifications can introduce to additive manufacturing. Indeed, the increased use of additive manufacturing to produce safety-critical parts magnifies the potential cost of failing parts beyond mere financial implications.

Although the `dr0wned` scenario involved sabotage at the service provider level, sabotage attacks are by no means restricted to direct attacks. As illustrated in the additive manufacturing workflow, other actors are indirectly involved in the manufacturing process, including electric power and feedstock suppliers. Yampolskiy et al. [49] have shown that modifications to physical commodities can also lead to the degradation of the manufactured products. Pope and Yampolskiy [26] have identified the impacts of power disturbances on the final products. Any of these methods could be leveraged in a sabotage attack.

Other exposed components in the additive manufacturing workflow are the software and firmware employed in the service provider infrastructure. Because they are frequently developed by third parties, their integrity can be compromised prior to system integration, via external network connections or pushed in by compromised updates and patches.

4. Liability Analysis Framework

Figure 3 presents the framework proposed for analyzing the liability incurred as a result of sabotage attacks on additive manufacturing.

The `dr0wned` scenario can be generalized and applied to other systems, including safety-critical systems in the automotive and aerospace industries. Failures of these systems can result in significant financial loss, serious injury and death. An injured party in such an incident could have recourse against the participants in the additive manufacturing workflow. The directly injured party could be the operator of a failed system who suffered property loss and/or physical injury. The indirectly injured party could be an innocent bystander with no connection to the additive manufacturing process or product.

An end user typically does not purchase a product directly from the manufacturer. Instead, retailers and resellers are often the final participants in the commercial distribution chain. This work does not consider the possibility of sabotage via part substitution or intentional damage at the retailer, reseller or physical carrier sites. Therefore, the retailer, reseller and physical carrier are grouped in with the end user at the consumer level. The liability analysis framework recognizes that any claim between these parties and the participants

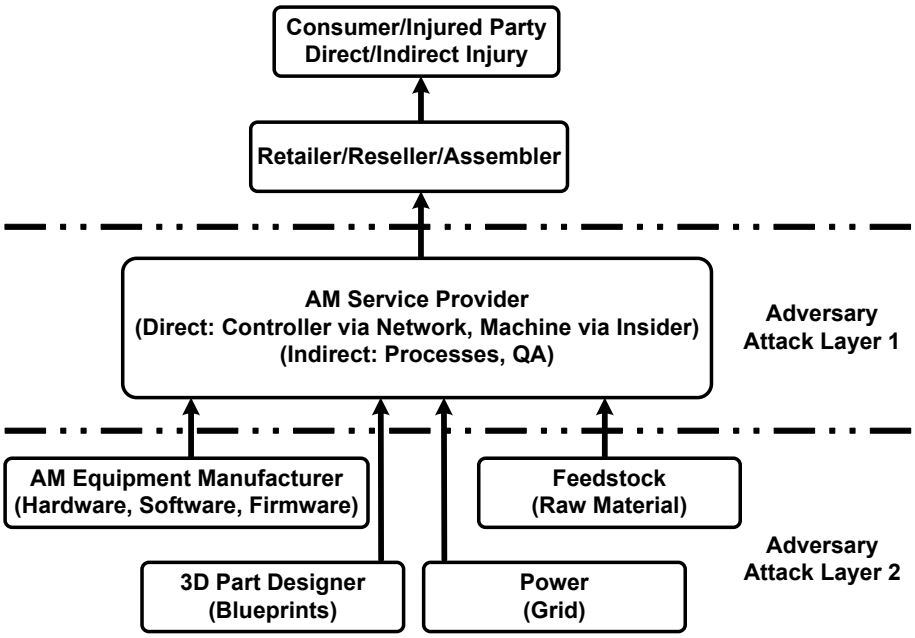

Figure 3. Liability analysis framework for sabotage attacks.

in the remainder of the additive manufacturing workflow would be governed by contractual indemnification processes, not personal injury liability.

A manufactured part is rarely an end product. Often, it is part of a multi-step assembly process that involves several business entities. Although part substitution is possible during this chain, it is not considered in this work. As with a retailer and reseller, between-party liability would be addressed as a part of the contractual relationship.

The manufacturing level is considered to be the first attack layer. An attack in this layer is similar to that perpetrated in the `dr0wned` study. What differentiates attacks in this layer is that they are the closest to the end user and can target specific end products. These attacks can be performed by modifying design files [4, 31, 51] or by compromising the additive manufacturing process [26, 30, 49, 50]. The attacks at this level are considered to operate in adversary attack layer 1.

An additive manufacturing service provider relies on a variety of physical and cyber commodities. These commodities include additive manufacturing equipment with the requisite firmware and software, object blueprints, feedstock and power supply. Any of these could be substituted or contaminated in a sabotage attack. At this level, the attack is farthest from the end user and cannot be targeted at a specific manufactured part [50]. Therefore, this layer is distinguished as the adversary attack layer 2.

5. Liability Analysis

This section analyzes the potential liability exposure in four cases – two potential litigants (i.e., parties who are eligible to sue): (i) end user victim; and (ii) bystander victim, for which there are two attack layers: (i) adversary attack layer 1; and (ii) adversary attack layer 2. The parties that could be held liable include the manufacturer, retailer, commodity supplier, service provider, merchant and members of the commercial distribution chain.

For each of the four cases, the following causes of action are considered:

- **Products Liability (Strict Liability):** The strict liability [43] cause of action is the easiest case to establish. The injured party has to demonstrate that the product was defective, that the defect made the product unreasonably dangerous for use or consumption, and that the liable party was in the commercial distribution chain.

- **Products Liability (Express Warranty):** The express warranty [37] cause of action requires an explicit assurance that was relied upon by the purchaser. Here, the injured party would have to demonstrate that the seller made a promise with regard to the product and that it factored in the decision to purchase the product. Absent a written agreement, this might be considered difficult to prove.

- **Products Liability (Implied Warranty):** The implied warranty [38] cause of action involves merchantability of average quality and ordinary purpose or a warranty that the product was fit for a particular purpose [39]. In the case of particular purpose, the injured party would have to demonstrate that the seller knew the purpose of the product and that the buyer relied on the seller to provide a suitable product. Given that additive manufacturing is increasingly used in the just-in-time and on-demand manufacturing of parts, this cause of action might be easier to prove for additive manufacturing than in the case of normal manufacturing.

- **Products Liability (Negligence):** For products liability negligence [42], the injured party has to establish a duty of care, a breach of duty and that the breach caused the injury. The focus in this situation is on the actions rather than the product, which renders the cause of action more difficult to prove.

- **Negligence in Tort:** Negligence in tort [41] differs from products liability negligence in that products liability examines the defendant's actions in terms of commercially-relevant standards as opposed to a non-commercial actor. Negligence in tort also requires an injured party to demonstrate that he or she was a foreseeable plaintiff.

The intentional torts – battery, assault, infliction of emotional distress and trespass to chattel – require an injured party to establish that there was an

Table 1. Strict liability (end user layer 1).

Strict Liability	**dr0wned Project**
Defective Product	STL file compromise
Unreasonably Dangerous	Midflight failure
Commercial Distribution Chain	Based on additive manufacturing workflow
Anyone Endangered	Flight path

intent to act. For battery [35], the intent is to harm. For assault [36], the intent is to create fear. For infliction of emotional distress [40], the intent is to cause upset. For trespass to chattel [44], the intent is to deprive someone of the use of property.

In the case of battery, the intent to harm can be the knowledge that harm is certain to occur. If the manufacturer does not take steps to protect the manufacturing environment, especially the network and software, it could be argued that the manufacturer knew that sabotage was possible and that harm would result from non-conforming parts that failed during flight. However, intent is often difficult to prove in product cases, which is why products liability is more often grounds for recovery. Products liability focuses on the product while the other causes of action focus on the defendant's actions and intent.

5.1 End User (Adversary Attack Layer 1)

This section discusses liability with regard to an end user victim in adversary attack layer 1.

Strict Liability. In the case of strict liability, the end user victim must establish that the product was defective and that the defect rendered the product unreasonably dangerous for use. Comparing the original file against the altered STL file can demonstrate the defect. Because the propeller failed, the drone crashed and injury resulted, it is possible to argue that the defective part was unreasonably dangerous to use in a drone and that the end user was endangered by the defect. To be held liable, the defendant must be in the commercial distribution chain. The additive manufacturing workflow establishes that the retailer and service provider are in the commercial distribution chain. Table 1 summarizes the products liability strict liability elements.

Express Warranty. In the case of express warranty, the injured end user has to prove the terms of the warranty and that the propeller failure demonstrated a breach of the warranty. Depending on the terms of an express warranty, part failure may not be sufficient to prove the breach. The defendant must be a seller, demonstrated by the additive manufacturing workflow and commercial transaction, while the plaintiff could be the buyer, a household

Table 2. Express warranty (end user layer 1).

Express Warranty	**dr0wned Project**
Terms	Transaction specific
Breach	Midflight failure
Seller	Based on additive manufacturing workflow
Buyer/Expected User	Transaction specific

member, guest or someone else expected to use, consume or be affected by the part. Table 2 summarizes the products liability express warranty elements.

Table 3. Implied warranty (end user layer 1).

Implied Warranty	**dr0wned Project**
Average Quality	Derived from design requirements
Fit for Use	STL file comparison
Seller	Based on additive manufacturing workflow
Buyer/Expected User	Transaction specific

Implied Warranty. Implied warranty involves merchantability or fit for a particular use. Merchantability requires that the part be of average quality and fit for ordinary purposes. The propeller failed the average quality and fit for particular use requirements due to premature fatigue. The quality and fit requirements were arguably captured in the design files; the failure to meet the requirements can be confirmed by comparing the executed files against the design files. Under implied warranty, the buyer relies on the seller to produce a conforming part and to protect the marketplace. The plaintiff can be any buyer, household member, guest or someone else expected to use, consume or be affected by the product. In the case of implied warranty, the defendant is a merchant in goods of that kind. Table 3 summarizes the products liability implied warranty elements.

Negligence. Key to products liability negligence is demonstrating a duty of care. Although a defendant might argue that standards are not established in the additive manufacturing industry, duty of care in the industry could be expected to combine manufacturing care with cyber security standards for the information technology infrastructure. The question would be whether the additive manufacturing service provider implemented available protections and defenses or those comparable with other cyber-physical systems, especially with regard to open-source software and network connectivity, as well as man-

Table 4. Negligence (end user layer 1).

Negligence	**dr0wned Project**
Reasonable Person	Analysis of security decisions
Breach	File compromise with failure
Manufacturer	Based on additive manufacturing workflow
Foreseeably Endangered	Flight path

ufacturing quality assurance for the purpose of detecting problems. Table 4 summarizes the products liability negligence elements.

Table 5. Negligence in tort (end user layer 1).

Negligence in Tort	**dr0wned Project**
Reasonable Person	Analysis of security decisions
Breach	File compromise with failure
Actual Cause	Sabotaged part failure
Legal Cause	Based on additive manufacturing workflow
Foreseeable	Flight path

Negligence in Tort. Negligence in tort has more components to establish for recovery. The reasonable person standard of care is owed to a foreseeable plaintiff. Negligence also requires demonstrating a breach of the duty of care and that the defendant's actions caused the injury. In the `dr0wned` attack, the modified file along with the destruction and injury would demonstrate the breach. Note that the cause must be actual and legal. Actual cause dictates that the injury would not have occurred, but for the retailer's or service provider's action in furnishing the sabotaged part. Legal cause requires a direct injury with no intervening cause or an indirect injury that was a foreseeable result. Table 5 summarizes the negligence elements.

5.2 Bystander (Adversary Attack Layer 1)

This section discusses liability with regard to a bystander victim in adversary attack layer 1.

Strict Liability. In the case of strict liability, the plaintiff is someone who was endangered by a defect. Thus, the bystander victim would use the same arguments as the end user victim to establish liability. Table 6 summarizes the products liability strict liability elements.

Table 6. Strict liability (bystander layer 1).

Strict Liability	**dr0wned Project**
Defective Product	STL file compromise
Unreasonably Dangerous	Midflight failure
Commercial Distribution Chain	Based on additive manufacturing workflow
Anyone Endangered	Flight path

Table 7. Express warranty (bystander layer 1).

Express Warranty	**dr0wned Project**
Terms	Transaction specific
Breach	Midflight failure
Seller	Based on additive manufacturing workflow
Expected to be Affected	Transaction and flight path

Express Warranty. In the case of express warranty, the plaintiff may be a guest or someone who is expected to be affected by a product. Thus, the injured bystander would use the same arguments as an end user victim to establish liability. However, the bystander may have greater difficulty in establishing the fact of a warranty depending on his or her relationship to the buyer. Table 7 summarizes the products liability express warranty elements.

Table 8. Implied warranty (bystander layer 1).

Implied Warranty	**dr0wned Project**
Average Quality	Derived from design requirements
Fit for Use	STL file comparison
Seller	Based on additive manufacturing workflow
Expected to be Affected	Transaction and flight path

Implied Warranty. As in the case of express warranty, the plaintiff can be a guest or someone who is expected to be affected by the product. Thus, the injured bystander would use the same arguments as an end user victim to establish liability. Table 8 summarizes the products liability implied warranty elements.

Negligence. The plaintiff in a products liability negligence case can be someone who has been foreseeably endangered. Therefore, the injured by-

Table 9. Negligence (bystander layer 1).

Negligence	**dr0wned Project**
Reasonable Person	Analysis of security decisions
Breach	File compromise with failure
Manufacturer	Based on additive manufacturing workflow
Foreseeably Endangered	Flight path

stander would need to establish that the additive manufacturing defendants could have foreseen injury to the bystander in addition to the actual user. It is arguable that the manufacturer could have foreseen that people other than the operator would be injured by a drone falling from the sky due to a sabotaged part, although other circumstances such as the relationship to the operator and operating location would be considered. After being established as a foreseeable plaintiff, the injured bystander could use the same products liability negligence arguments as the end user plaintiff. Table 9 summarizes the products liability negligence elements.

Table 10. Negligence in tort (bystander layer 1).

Negligence in Tort	**dr0wned Project**
Reasonable Person	Analysis of security decisions
Breach	File compromise with failure
Actual Cause	Sabotaged part failure
Legal Cause	Based on additive manufacturing workflow
Foreseeable	Flight path

Negligence in Tort. In the case of negligence in tort, the reasonable standard of care is owed to the foreseeable plaintiff. In the `dr0wned` sabotage attack, it is arguable that a machine that fell from the sky and resulted in injury to an innocent bystander would violate the reasonable person standard, especially since the sabotage occurred under the control of the manufacturer. It is also arguable that the bystander is a foreseeable plaintiff. The additive manufacturer produced a propeller used in a flying machine that could cause indiscriminate harm if it fell from the sky upon failure. Demonstrating the breach could include showing a failure to use available means to prevent and detect the sabotage, along with a comparison of the original and actual files. In the event of a compromised jet nozzle resulting in potentially more loss of life and property damage, competing concerns of social utility and societal loss distribution would have to be balanced. Table 10 summarizes the negligence elements.

Table 11. Strict liability (end user layer 2).

Strict Liability	**dr0wned Project**
Defective Product	Comparison of design specifications against compromised commodities
Unreasonably Dangerous	Midflight failure
Commercial Distribution Chain	Based on additive manufacturing workflow
Anyone Endangered	Untargeted attack and flight path

5.3 End User (Adversary Attack Layer 2)

This section discusses liability with regard to an end user victim in adversary attack layer 2.

Strict Liability. In attack layer 2, the defect is introduced via one of the cyber or physical commodities. However, under strict liability, the focus is on the product and whether its defect rendered it unreasonably dangerous for use rather than the source of the defect. In the `dr0wned` scenario, it would be the same for end user recovery whether the fatigue was introduced in layer 1 by the altered STL file or in layer 2 by contaminated feedstock, power fluctuations or firmware updates. As such, liability against the manufacturer would be established as with the layer 1 attack. The layer 2 attack introduces an additional liable party, the commodity supplier, which the injured party could argue is part of the commercial distribution chain. Table 11 summarizes the products liability strict liability elements.

Express Warranty. In the case of express warranty, the focus is on the warranty and the breach. For a layer 2 attack, the terms of the warranty would determine whether the source of the defect was relevant to the cause of action. Depending on the warranty, a layer 2 attack might not necessarily excuse the manufacturer from liability while also exposing the commodity supplier. However, the greater the distance of the end user from the source of the defect, the more complicated it would be to establish the necessary relationship or that the commodity supplier is a liable party. Table 12 summarizes the products liability express warranty elements.

Implied Warranty. As in the case of strict liability, the cause of action in implied warranty focuses on the product and the defect instead of the source of the defect. The failure of the propeller to meet average quality or fit for a particular use standard is independent of the defect's origin. The buyer's reliance on the manufacturer to produce a conforming part and to protect the marketplace has not changed. Rather, the manufacturer's placement between the end user and the source of the sabotage underscore its role in protecting

Table 12. Express warranty (end user layer 2).

Express Warranty	**dr0wned Project**
Terms	Transaction specific
Breach	Midflight failure
Seller	Based on additive manufacturing workflow
Buyer/Expected User	Transactional distance

Table 13. Implied warranty (end user layer 2).

Implied Warranty	**dr0wned**
Average Quality	Derived from design specifications
Fit for Use	Specified commodity quality
Seller	Based on additive manufacturing workflow
Buyer/Expected User	Transactional distance

the marketplace. In addition to not excusing the manufacturer, the layer 2 attack exposes the commodity supplier to liability because the end user can be categorized as affected by the defect regardless of origin. For example, if the `dr0wned` defect was created when the contaminated material did not fuse, then the end user was affected by the contaminated feedstock. Table 13 summarizes the products liability implied warranty elements.

Negligence. The duty of care to the end user in a layer 2 attack might arguably include screening activities at the commodity supplier and manufacturer levels. In exercising due care, the commodity supplier could be expected to screen cyber and physical commodities for flaws, bugs and other compromises prior to shipping. The manufacturer could be expected to conduct screening at intake to detect layer 2 compromises. In the case of feedstock, it is common for the manufacturer to rely on the supplier's characterization. In the `dr0wned` sabotage scenario, this would enable contaminated feedstock to compromise the propeller leading to the drone failure and injury to the end user. Table 14 summarizes the products liability negligence elements.

Negligence in Tort. In the case of negligence in tort, the injured end user would have to show standing as a foreseeable plaintiff and that the liable parties violated a reasonable person standard of care. In a layer 2 attack, it is arguably foreseeable that harm would reach the end user because sabotage at the commodity supplier level cannot be targeted, but could impact anyone along the manufacturing process chain up to and including the end user. For the reasonable person standard, the injured user could include prevention

Table 14. Negligence (end user layer 2).

Negligence	**dr0wned Project**
Reasonable Person	Analysis of screening/security decisions
Breach	Commodity compromise with failure
Commercial Seller	Based on additive manufacturing workflow
Foreseeably Endangered	Untargeted attack and flight path

Table 15. Negligence in tort (end user layer 2).

Negligence in Tort	**dr0wned Project**
Reasonable Person	Analysis of screening/security decisions
Breach	Commodity compromise with failure
Actual Cause	Sabotaged part failure
Legal Cause	Based on additive manufacturing workflow
Foreseeable	Untargeted attack and flight path

and detection measures employed in other similar industries to demonstrate protections against and attempts to detect compromised cyber and physical supplies. The measures could also be used to demonstrate the reasonableness of deployment at the manufacturing level given the susceptibility of cyber and manufacturing systems to attack. The cause must be actual and legal. Actual cause dictates that the injury would not have occurred but for the sabotage, which can be established with a showing that the parts do not fail under the same circumstances and that the injury results from the part failure. Legal cause requires a direct injury with no intervening cause or an indirect injury that was a foreseeable result. The injured party would argue that, although the various steps of the process chain might appear to be intervening causes, the part failure is a foreseeable result when a compromise disrupts the manufacturing process. Table 15 summarizes the negligence elements.

5.4 Bystander (Adversary Attack Layer 2)

This section discusses liability with regard to a bystander victim in adversary attack layer 2.

Strict Liability. For the bystander victim of a layer 2 sabotage attack, the focus is still on the product and whether the bystander victim was endangered by the defect. The bystander victim would use the same arguments as the end user victim of a layer 1 attack to establish liability. With the focus on the product, the source of the defect would be irrelevant to the manufacturer's exposure to bystander liability. The commodity supplier would also be exposed

Table 16. Strict liability (bystander layer 2).

Strict Liability	**dr0wned Project**
Defective Product	Comparison of design specifications against compromised commodities
Unreasonably Dangerous	Midflight failure
Commercial Distribution Chain	Based on additive manufacturing workflow
Anyone Endangered	Untargeted attack and flight path

to strict liability recovery, although the supplier could attempt to argue that it was not part of the commercial distribution chain or that its sabotaged contribution to the product was not the source of the defect that injured the bystander. Table 16 summarizes the products liability strict liability elements.

Table 17. Express warranty (bystander layer 2).

Express Warranty	**dr0wned Project**
Terms	Transaction specific
Breach	Midflight failure
Seller	Based on additive manufacturing workflow
Expected to be Affected	Transactional distance and flight path

Express Warranty. As in the case of a layer 1 attack, the bystander victim could use the same arguments as the end user because the express warranty extends to anyone who is expected to be affected by a product. The layer 2 attack would pose the same challenges to the bystander as it does to an end user with regard to the warranty terms and the ability to include or extend the warranty to the commodity supplier. Table 17 summarizes the products liability express warranty elements.

Implied Warranty. Since the bystander victim could be someone who is expected to be affected by the product, the same layer 2 arguments for the end user with regard to implied warranty could be applied by the bystander. The commodity supplier could argue that the product was the sabotaged commodity instead of the compromised propeller and, as such, the bystander was not in the expected class of user. However, the commodity supplier has a role in protecting the marketplace, as does the manufacturer, which is the underlying social policy for implied warranty liability. Thus, the manufacturer and the commodity supplier arguably would be exposed to implied warranty liability because the bystander was injured as a result of the layer 2 sabotage attack. Table 18 summarizes the products liability implied warranty elements.

Table 18. Implied warranty (bystander layer 2).

Implied Warranty	**dr0wned Project**
Average Quality	Derived from design specifications
Fit for Use	Specified commodity quality
Seller	Based on additive manufacturing workflow
Expected to be Affected	Transactional distance and flight path

Table 19. Negligence (bystander layer 2).

Negligence	**dr0wned**
Reasonable Person	Analysis of screening/security decisions
Breach	Commodity compromise with failure
Commercial Seller	Based on additive manufacturing workflow
Foreseeably Endangered	Untargeted attack and flight path

Negligence. The foreseeability of a bystander victim as someone endangered by the sabotaged product is again an issue with this cause of action. As in the case of a layer 1 attack, it is arguable that the manufacturer could have foreseen that individuals other than the operator could be injured by a drone falling from the sky due to a sabotaged part. It is also arguable that the commodity supplier could have foreseen that anyone up the workflow, including bystanders, could be injured by the sabotage of items under its control. Due to the untargeted nature of a layer 2 attack, it is perhaps even more arguable that an unsuspecting bystander would be endangered. After a bystander victim is established as a foreseeable plaintiff, the bystander could use the same products liability negligence arguments as the end user plaintiff to hold the manufacturer and commodity supplier liable. Table 19 summarizes the products liability negligence elements.

Negligence in Tort. In the case of negligence in tort, the liability argument for a layer 2 sabotage would resemble that of an end user victim because the attack was indiscriminate and could foreseeably have injured anyone after the point of the compromise. If the defendant claims that the sheer indiscriminate nature contradicts any foreseeability, the bystander could argue that it is exactly why he/she is a foreseeable plaintiff and why the reasonable person standard would examine what measures could and should have been deployed to prevent indiscriminate injury. The nature of the control of the manufacturer and commodity supplier of the component and the preventative measures, along with the indiscriminate nature and extent of the harm, combine to form the basis for meeting the foreseeable plaintiff standard and the breach of a reason-

Table 20. Negligence in tort (bystander layer 2).

Negligence in Tort	**dr0wned Project**
Reasonable Person	Analysis of screening/security decisions
Breach	Commodity compromise with failure
Actual Cause	Sabotaged part failure
Legal Cause	Based on additive manufacturing workflow
Foreseeable	Untargeted attack and flight path

able person standard of care. As in the case of the bystander in layer 1 and end user in layer 2, the defendants could argue that intervening events and actions affected the actual and legal cause elements. However, traceability from the introduction of sabotage (by power fluctuations, compromised firmware or contaminated feedstock) to the end product would establish actual cause. The fact that injury resulted from a failed compromised part that caused the drone to fall from the sky would establish the legal cause. If the compromise was not traceable to the original sabotage, then the injured bystander could argue that it was further indication that the reasonable person standard was violated because the commodity supplier did not sufficiently audit its processes and materials and the service provider did not sufficiently audit its supplies. Table 20 summarizes the negligence elements.

6. Discussion

This chapter has discussed the financial liability of the entire additive manufacturing supply chain in the event of a sabotage attack. However, there are some topics that are out of scope, but still bear mentioning. This section briefly discusses the financial liability between participants in the manufacturing process, corporate criminal liability and nation-state actors.

6.1 Liability between Process Chain Elements

Three areas should be considered when making decisions about security investments to combat sabotage attacks: (i) liability to external parties; (ii) liability between parties; and (iii) shifting risk through insurance. Liability to external parties has been covered in detail. This section briefly discusses the remaining two areas.

Liability between the participants in the additive manufacturing chain, from supplier to manufacturer, can be considered to be a contractual situation. It is anticipated that workflow component liability would be governed by the contracts between the parties [9, 24]. Insurance adds another factor to liability between the participants in the additive manufacturing workflow because it shifts the risk outside the workflow [17, 34]. Liability between parties and insurance are both considerations for additive manufacturing components with

regard to liability exposure and the detection and prevention of 3D printer sabotage attacks.

6.2 Corporate Criminal Liability

Criminal liability is not likely for corporate behavior. An exception was the 2010 Deepwater Horizon explosion that killed eleven people and spilled millions of gallons of oil into the Gulf of Mexico [28]. The company (BP) plead guilty to fourteen criminal charges and paid $1.256 billion in fines [18]. By comparison, BP was levied $18.7 billion in fines for environmental and economic damage [29]. Company employees were also charged, but the harshest sentence was probation [14].

If a corporation is to be held criminally liable for an act by an employee, then the act must be in the scope of employment, it must benefit the company and there must be intent that can be imputed to the company [10, 13]. An act can be a decision to omit quality control. It can also be a decision not to implement security measures (e.g., based on risk analysis). For a corporation to be held liable in a sabotage attack, intent would again be an issue as in the civil liability analysis presented in this chapter. Additionally, the act of sabotage would not normally be in the corporation's interest.

6.3 Nation-State Actors

If a nation-state actor were to launch a sabotage attack, the Foreign Sovereign Immunities Act would make it difficult to pursue liability. There is, however, a commercial activity exemption that could be invoked for a civil cause of action [3, 15]. In this case, attribution is required. Based on the prior cases, tracing an attack on a cyber system has proven to be difficult [3, 6, 7]. The additive manufacturing workflow adds complexity due to the number of participants and the avenues of attack. Given the distributed nature of cyber systems and additive manufacturing environments, there is a strong likelihood that the saboteur would have launched a remote attack, which would raise jurisdictional issues. Trans-jurisdictional investigation and prosecution could be considered to be insurmountable problems [3, 7, 25]. Beyond the technical limitations related to attribution and jurisdiction, political considerations impose additional restrictions because governments generally avoid exposing their investigative capabilities.

7. Conclusions

The `dr0wned` study [4] demonstrated the feasibility and impact of a sabotage attack on additive manufacturing. The question now is not if, but when such attacks will occur.

This chapter has analyzed liability exposure arising from sabotage attacks on additively-manufactured functional parts. It established the sabotage attack layers, developed a framework for analyzing liability for sabotage attacks

on functional parts and analyzed the civil liability exposure of the additive service provider and commodity suppliers in the event of an attack that results in injury to an end user and/or bystander. The analysis reveals that the parties are exposed to potential liability that would result in expensive investigations and defense costs regardless of whether or not they are ultimately held responsible and incur financial penalties. Additionally, additive manufacturing service providers and the nascent industry would suffer reputation loss as a result of injury-causing accidents. This would be especially true if the additive manufacturing industry is viewed as being more susceptible to sabotage attacks compared with the traditional manufacturing industry or is portrayed as failing to implement prevention and detection techniques in pursuit of profit. It is, therefore, important that all the additive manufacturing actors conduct or re-evaluate their cost-benefit analyses and invest in security measures.

References

[1] M. Albakri, L. Sturm, C. Williams and P. Tarazaga, Non-destructive evaluation of additively-manufactured parts via impedance-based monitoring, *Proceedings of the Twenty-Sixth International Solid Freeform Fabrication Symposium*, pp. 1475–1490, 2015.

[2] American Society for Testing and Materials, Standard Terminology for Additive Manufacturing Technologies, ASTM F2792-12a, West Conshohocken, Pennsylvania, 2012.

[3] P. Anderson, Cyber attack exception to the Foreign Sovereign Immunities Act, *Cornell Law Review*, vol. 102(4), pp. 1087–1114, 2017.

[4] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin and Y. Elovici, `dr0wned` – Cyber-physical attack with additive manufacturing, *Proceedings of the Eleventh USENIX Workshop on Offensive Technologies*, 2017.

[5] N. Berkowitz, Strict liability for individuals? The impact of 3-D printing on products liability law, *Washington University Law Review*, vol. 92(4), pp. 1019–1053, 2015.

[6] S. Brenner, At light speed: Attribution and response to cybercrime/terrorism/warfare, *Journal of Criminal Law and Criminology*, vol. 97(2), pp. 379–476, 2007.

[7] C. Brown, Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice, *International Journal of Cyber Criminology*, vol. 9(1), pp. 55–119, 2015.

[8] L. Columbus, 2015 roundup of 3D printing market forecasts and estimates, *Forbes*, March 31, 2015.

[9] P. Comerford and E. Belt, 3DP, AM, 3DS and products liability, *Santa Clara Law Review*, vol. 55(4), pp. 821–836, 2015.

[10] C. Doyle, Corporate Criminal Liability: An Overview of Federal Law, Congressional Research Service, Washington, DC, 2013.

[11] N. Engstrom, 3-D printing and products liability: Identifying the obstacles, *University of Pennsylvania Law Review Online*, vol. 162, pp. 35–41, 2013.

[12] W. Frazier, Metal additive manufacturing: A review, *Journal of Materials Engineering and Performance*, vol. 23(6), pp. 1917–1928, 2014.

[13] A. Geraghty, Criminal Corporate Liability, Seventeenth Survey of White Collar Crime, *American Criminal Law Review*, vol. 39, pp. 327–354, 2002.

[14] J. Gill, Disaster prosecution is, well, a disaster, *The New Orleans Advocate*, March 12, 2016.

[15] S. Gilmore, Suing the surveillance states: The (cyber) tort exception to the Foreign Sovereign Immunities Act, *Columbia Human Rights Law Review*, vol. 46(3), pp. 227–287, 2014.

[16] T. Kellner, An epiphany of disruption: GE additive chief explains how 3D printing will upend manufacturing, *GE Reports*, November 13, 2017.

[17] M. Koch and B. Stansbury, 3-D printing: Innovation, opportunities and risk, *Law360*, February 24, 2016.

[18] C. Krauss and J. Schwartz, BP will plead guilty and pay over $4 billion, *The New York Times*, November 15, 2012.

[19] E. Malloy, Three-dimensional printing and a laissez-faire attitude towards the evolution of the products liability doctrine, *Florida Law Review*, vol. 68(4), pp. 1199–1226, 2016.

[20] Markets and Reports, 3D Printing Market Trends: Global Market Growth and Forecasting 2015–2020, DART Consulting, Bangalore, India, October 10, 2015.

[21] S. Moore, P. Armstrong, T. McDonald and M. Yampolskiy, Vulnerability analysis of desktop 3D printer software, *Proceedings of the IEEE Resilience Week*, pp. 46–51, 2016.

[22] S. Moore, W. Glisson and M. Yampolskiy, Implications of malicious 3D printer firmware, *Proceedings of the Fiftieth Hawaii International Conference on System Sciences*, pp. 6089–6098, 2017.

[23] H. Nielson, Manufacturing consumer protection for 3-D printed products, *Arizona Law Review*, vol. 57(2), pp. 609–622, 2015.

[24] L. Osborn, Regulating three-dimensional printing: The converging worlds of bits and atoms, *San Diego Law Review*, vol. 51, pp. 553–621, 2014.

[25] E. Podgor, Cybercrime: National, transnational or international? *Wayne Law Review*, vol. 50, pp. 97–108, 2004.

[26] G. Pope and M. Yampolskiy, A hazard analysis technique for additive manufacturing, presented at the *Better Software East Conference*, 2016.

[27] P. Reddy, The legal dimension of 3D printing: Analyzing secondary liability in additive layer manufacturing, *Columbia Science and Technology Law Review*, vol. XVI, pp. 222–247, 2014.

[28] C. Robertson and C. Krauss, Gulf spill is the largest of its kind, scientists say, *The New York Times*, August 2, 2010.

[29] C. Robertson, J. Schwartz and R. Perez-Pena, BP to pay $18.7 billion for Deepwater Horizon oil spill, *The New York Times*, July 2, 2015.

[30] A. Slaughter, M. Yampolskiy, M. Matthews, W. King, G. Guss and Y. Elovici, How to ensure bad quality in metal additive manufacturing: In-situ infrared thermography from the security perspective, *Proceedings of the Twelfth International Conference on Availability, Reliability and Security*, article no. 78, 2017.

[31] L. Sturm, C. Williams, J. Camelio, J. White and R. Parker, Cyber-physical vulnerabilities in additive manufacturing systems, *Proceedings of the Twenty-Fifth International Solid Freeform Fabrication Symposium*, pp. 951–963, 2014.

[32] L. Sturm, C. Williams, J. Camelio, J. White and R. Parker, Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects, *Journal of Manufacturing Systems*, vol. 44(1), pp. 154–164, 2017.

[33] Technovelgy, Plastic Constructor (3D Printer) (`www.technovelgy.com/ct/content.asp?Bnum=2445`), 2017.

[34] A. Thierer and A. Marcus, Guns, limbs and toys: What future for 3D printing? *Minnesota Journal of Law, Science and Technology*, vol. 17(2), pp. 805–854, 2016.

[35] Thomson Reuters Editorial Staff, § 87 Battery, *American Jurisprudence Second*, vol. 6, 2017.

[36] Thomson Reuters Editorial Staff, § 90 Causing apprehension, *American Jurisprudence Second*, vol. 6, 2017.

[37] Thomson Reuters Editorial Staff, § 631 Express warranties, *American Jurisprudence Second*, vol. 63, 2017.

[38] Thomson Reuters Editorial Staff, § 676 Implied warranties, *American Jurisprudence Second*, vol. 63, 2017.

[39] Thomson Reuters Editorial Staff, § 676 Implied warranty of fitness for particular purpose, *American Jurisprudence Second*, vol. 63, 2017.

[40] Thomson Reuters Editorial Staff, § 37 Intentional infliction of emotional distress, *American Jurisprudence Second*, vol. 74, 2017.

[41] Thomson Reuters Editorial Staff, § 1 Negligence, *American Jurisprudence Second*, vol. 57A, 2017.

[42] Thomson Reuters Editorial Staff, § 207 Negligence liability, *American Jurisprudence Second*, vol. 63, 2017.

[43] Thomson Reuters Editorial Staff, § 508 Strict liability in tort, *American Jurisprudence Second*, vol. 63, 2017.

[44] Thomson Reuters Editorial Staff, § 11 Trespass to chattel, *American Jurisprudence Second*, vol. 75, 2017.

[45] S. Wang, When classical doctrines of products liability encounter 3D printing: New challenges in the new landscape, *Houston Business and Tax Law Journal*, vol. 16, pp. 104–126, 2016.

[46] Wohlers Associates, Wohlers Report 2017: 3D Printing and Additive Manufacturing State of the Industry, Annual Worldwide Progress Report, Fort Collins, Colorado, 2017.

[47] M. Yampolskiy, W. King, J. Gatlin, S. Belikovetsky, A. Brown, A. Skjellum and Y. Elovici, Security of additive manufacturing: Attack taxonomy and survey, *Additive Manufacturing*, vol. 21, pp. 431–457, 2018.

[48] M. Yampolskiy, W. King, G. Pope, S. Belikovetsky and Y. Elovici, Evaluation of additive and subtractive manufacturing from the security perspective, in *Critical Infrastructure Protection XI*, M. Rice and S. Shenoi (Eds.), Springer, Cham, Switzerland, pp. 23–44, 2017.

[49] M. Yampolskiy, L. Schutzle, U. Vaidya and A. Yasinsac, Security challenges of additive manufacturing with metals and alloys, in *Critical Infrastructure Protection IX*, M. Rice and S. Shenoi (Eds.), Springer, Cham, Switzerland, pp. 169–183, 2015.

[50] M. Yampolskiy, A. Skjellum, M. Kretzschmar, R. Overfelt, K. Sloan and A. Yasinsac, Using 3D printers as weapons, *International Journal of Critical Infrastructure Protection*, vol. 14, pp. 58–71, 2016.

[51] S. Zeltmann, N. Gupta, N. Tsoutsos, M. Maniatakos, J. Rajendran and R. Karri, Manufacturing and security challenges in 3D printing, *Journal of the Minerals, Metals and Materials Society*, vol. 68(7), pp. 1872–1881, 2016.