以 3D 打印机作为武器

摘要：增材制造，也被称为 3D 打印，是一种将在关键制造领域发挥重要作用的变革性的制造技术。工业级的三维打印机越来越多地用于为重要系统制造功 能性部件。但是，由于 3D 打印机依赖于计算机化而容易受到各种攻击。更重要的是，3D 打印机本身不是目标，而是将该打印机作为启动后续攻击的临时点。例如，对手可以控制 3D 打印机以便操纵制造部件的机械特性。如果制造的部件用于喷气发动机或者在其他安全关键系统中，它们可能危及人类生命，破坏关键基础设施资产并产生重大的经济和社会影响。

本文分析了对手将被控制的增材制造设备“武器化”以造成动能，核，生物，化学或网络损害的能力。特别地，本文介绍了增材制造工作流程中容易受到攻击的元素的类别（分类法），受到攻击的元素将会被控制，被控制之下将产生的带有武器效果的影响。本文也讨论了这些分类法之间的关系。最后，描述了 3D 打印机的武器化可能性。

第 1 章　引言

增材制造（AM），也称为添加层制造或 3D 打印，通过添加薄层将物体从二维构建到所需的三维形式，逐步创建物体[80] 。与传统制造相比，增材制造具有多项技术和经济优势。这包括及时生产和按需生产，可按装配线的需要来制造零件，缩短设计到产品的时间，可以生产具有复杂内部几何形状和针对各种应用领域优化的机械性能的功能部件。

增材制造技术的市场渗透具有巨大的潜力。Wohlers Associates [80] 在 2014 年报告称，增材制造业的收入为 41 亿美元，其中 29％的制造物体被用作功能部件。根据 NIST[72，73] ，增材制造技术将在 2031 年至 2038 年间达到其市场潜力的　50％，在 2029 年至 2031 年期间的收入约为 500 亿美元。

随着增材制造成为一种变革性技术[10] ，许多机构和公司正在研究该技术的应用。SpaceX 使用增材制造为其最新的龙宇宙飞船　生产发动机舱[27] 。通用电气建造了复杂的支架，比传统的结构件重量减少了 80％[29] 。NASA 创造了一种专为高负荷和温度梯度　设计的火箭喷射器 [60]。荷兰公司 DUS Architects 计划使用增材制造来印刷整个三层住宅[19]。

巨大的市场潜力以及增材制造技术的经济，地缘政治和其他影响[6,9,35]将不可避免地引起对手的注意，从个人到国家行为者。由于 3D 打印机依赖于计算机化，因此容易受到各种攻击。这是对“野外”检测到的网络物理系统的一系列攻击以及研究文献中假设的攻击所支持的。其中包括对工业控制系统的攻击[8,25，41，66] ，最先进的技术汽车[14,39]和无人驾驶和载人航空系统[26,81,84]。所有这些例子都指向这样一个结论结论：对增材制造系统的攻击和增材制造技术的滥用就在眼前。

本文探讨了如何将 3D 打印机误用为武器。它没有讨论能够使对手控制制造过程的特定网络或物理攻击。相反，它首先要确定可能被成功攻击破坏的元素。在此之后，本文讨论了对被控制元素可以行使的操纵。最后，该文件强调了这些操纵的效果，并证明它们与几类武器产生的效果相当。

第 2 章　相关工作

本节讨论增材制造安全性，并概述了一些与安全相关的（攻击）分类法。

2.1. 增材制造的安全性

目前关于增材制造安全性的文献非常稀少。然而，最近的文章[67,77]表明人们越来越意识到侵犯知识产权的威胁以及对增材制造系统和基础设施的破坏。

在文献中所讨论的知识产权保护的各方面包括开放挑战[18,53]，知识产权法应用到增材制造[7]，嵌入恶意软件在源文件窃取知识产权（例如，ACAD／Medre.A 蠕虫[23]），外包情景中知识产权保护的技术挑战[82]以及水印技术在检测假冒伪劣部分方面的应用[46]。

攻击增材制造基础设施造成物理损害的能力是一个主要问题[83]。最近的几个出版物分享了这一评估[52,67,68,87]。Sternstein[67]讨论了由于管理不善导致 3D 打印机爆炸的可能性；这样的事件实际上发生在 2013 年 11 月[56]。

Yampolskiy 等[87]已经进行了关于材料科学和机械工程文献的广泛调查并就对手影响被制造物体的物理特性的能力提供了定性分析。他们还列出了可能被操纵的金属打印机的制造参数，以及它们对制造零件的微观结构的影响，于是也就影响到这些零件的物理特性。Frazier 在对与增材制造相关的材料科学文献的调查中得出了类似的结论[28]，该调查重点关注影响制造零件质量的因素。

例如，考虑一下流行的粉末床融合过程[17,28,87]。在该过程中，粉末形式的源材料层（金属或聚合物）分布在腔室中。该层通过热源（激光或电子束）熔化，该热源熔化 3D 物体的下一切片的轮廓。该粉末分布和融合序列逐层重复。许多因素影响粉末床熔合过程。这些因素包括粉末特性（材料，形状，规律性和尺寸）[24,44,64]，热源及其性质（电子束或激光，直径，强度/材料和热源之间的距离）[48]，真空或惰性气体使用[3,30]，机器中机构的精度（控制室，热源位置和热源方向）[87]，支撑结构[80]，熔化模式[5]和液态和固态之间的过渡次数[37,38,76]。增材制造参数与被制造零件的物理特性之间的量化的相关关系是一个活跃的研究领域。例如，DARPA[70]最近宣布了其开放式制造计划，该计划旨在开发一个基于制造参数预测零件性能的模型。

文献[68]中提供了实验证据证明攻击者可以操纵源立体光刻（STL）文件并插入空隙（即空腔）以降低被制造物体的抗拉强度。类似地，对物体描述的操作可以改变被制造零件的尺寸[79,87]。但是，对源文件的操作只能更改物体几何形状。

2.2.攻击分类法

目前，尚未针对增材制造安全性制定攻击分类法。然而，已经发布了许多网络安全分类法，其中一些可用于建立增材制造领域的分类法。

Yampolskiy 等[85] 指出“分类学”是一个很宽泛的术语。该术语可以指单类别分类，多维表征或多维描述。本文建立了单一类别的分类法，通常表示为树状结构。例子包括对无线安全威胁[78],网络基础设施攻击[11]和分布式拒绝服务攻击[50]进行分类的分类法。维恩图也被用来表达单一类别的分类法;一个例子是对嵌入式系统的攻击特征 [61]。有兴趣的读者可以参考文献[31]来了解一些突出的分类法并讨论它们的局限性。

一些研究人员根据其属性，威胁和手段对可靠性和安全性的概念进行了分类[4,42]。Avizienis 等。[4] 特别引入了几种与本文相关的技术。可以将故障类别的可能组合视为分类法元素的交叉产物;Avizienis 及其同事将此表示为矩阵和树结构。错误传播也是在一个具有复杂的依赖关系的系统中的效应传播的因果链条一个很好的例子。

与网络物理系统相关的关键分类包括工业关键基础设施中的相互依赖性[32,62]以及对 SCADA 系统的攻击[20,36,88]。

第 3 章　背景

本节介绍增材制造工作流程。此外，还重点突出增材制造中最具代表性的材料和应用领域，包括电子，人体组织，食品和药品的打印。

3.1. 增材制造工作流程

图 3.1 显示了增材制造中涉及的参与者之间的相互作用。增材制造系统 - 以下也称为 3D 打印机 - 通常由原始设备制造商（OEM）和第三方供应商构建和提供。2014 年，13 个国家的 49 家系统制造商生产和销售工业级增材制造设备，估计有数百家小公司提供台式 3D 打印机[80] 。用户社区经常为 3D 打印机中的嵌入式控制器开发和发布固件更新，并为用于提交的“控制器计算机”进行软件更新并控制制造业工作。这些个人计算机还用于将固件更新应用于增材制造设备。

要打印的 3D 物体通常使用立体光刻（STL）格式[34]或增材制造文件（AMF）格式[16,43]，它们代表计算机辅助设计的“切片”版本（CAD ）3D 物体的模型。基于存储在 STL 或 AMF 文件中的 3D 物体描述，控制器计算机将命令发送到产生指定物体的 3D 打印机。这些命令定位建筑平台和喷嘴，调整平台温度等，通常编码为 G 代码 [21] ,这是一种常用于计算机辅助制造（CAM）的语言。

增材制造工艺需要源材料。美国材料与试验协会（ASTM）国际委员会 F42 关于增材制造技术已经批准了七种增材制造工艺类别 [80] 。这些过程在支持的源材料（例如，聚合物或金属），源材料分布的手段（例如，粉末床或喷嘴），热源（例如，激光，电子束或电弧）等方面不同。

在粉末床熔合（PBF）工艺中，粉末形式的薄的源材料层（通常是金属或聚合物）分布在粉末床中。该层通过热源（激光或电子束）熔化，该热源熔化 3D 物体的切片的轮廓； 这种粉末分布和融合序列是逐层重复的。在该过程中，只有一小部分分布在床中的粉末被熔化以产生所产生的物体。未使用的粉末可以回收利用以减少浪费，从而降低生产成本。但是，因为残留的粉末会暴露在高温下，它的性质可能会改变 - 例如，金属颗粒可能聚集成大的簇。由于这会影响所制造的 3D 物体的机械性能，因此通常将重复使用的粉末过筛并与“原始”粉末混合，其比例将负面影响降低到可接受的水平。

根据增材制造工艺，源材料和零件几何形状，生产工作流程可以包括图 3.1 中未示出的几个步骤。两个重要方面是支撑结构和后处理，这两者都会对印刷部件的质量产生重大影响。

打印具有复杂几何形状的零件需要支撑结构 - 这些结构主要用于防止悬垂的下垂。当使用金属和合金进行印刷时，支撑结构材料由于其在热分布　中的作用而对部件质量具有显着影响 [40]。在打印部件之后，通常移除并丢弃支撑结构。

在金属部件的生产过程中经常需要后处理。具体而言，通常需要热等静压（HIP）来消除残留的内部孔隙并提高印刷物的机械性能[28]。在 Ti-6Al-4　　V 合金的情况下，后处理涉及 100MPa 和 926° C　的热等静压循环 2 至 4 小时，然后炉冷却低于 427° C　[28]　。表面光洁度也可以通过提供裂纹起点[12] 对疲劳寿命等性能产生重大影响。

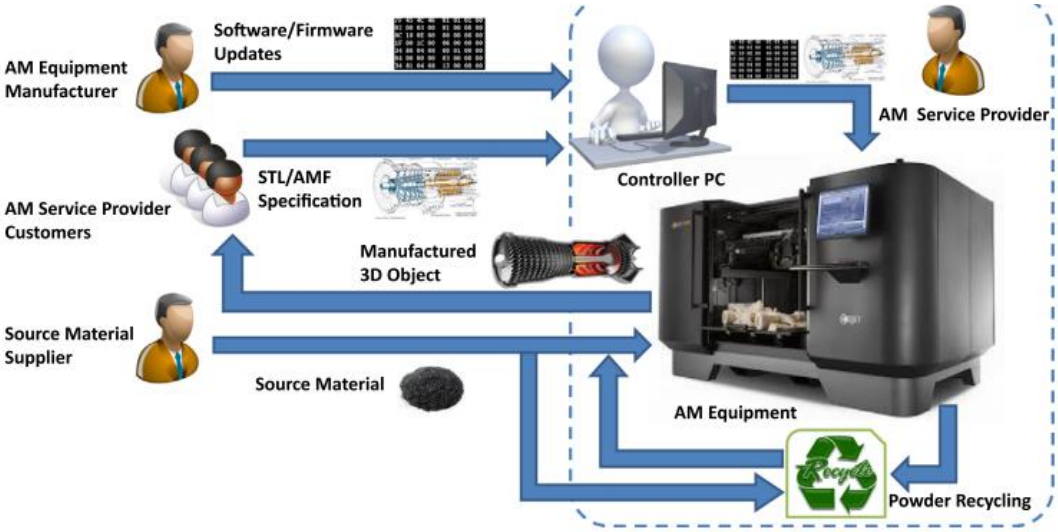

图 3.1 增材制造的工作流程

第 4 章　材料和应用领域

制造部件的应用领域高度依赖于使用的不同源材料可实现的能力。实际上，支持的源材料和应用领域的种类在不断扩大。根据 Wohlers 报告（一项关于增材制造业全球进展的重要年度调查）[80]，增材制造材料的两大类是塑料和金属。

塑料（或聚合物）是最大的一组增材制造源材料，具有多种性能，包括颜色，透明度，拉伸强度，刚性和生物相容性。材料范围从极硬塑料到橡胶状弹性体。由于具有广泛的可实现性能，3D 打印塑料物体的应用领域包括汽车和航空航天工业中的模型和功能部件。

增材制造设备支持的金属和合金清单包括不锈钢，钛，铝合金，金和银。应用领域根据材料和材料可实现的特性而变化。金属用于生产从手表外壳到整个喷气发动机的功能部件[65]。

生物相容材料（塑料和金属）可用于生产定制的医疗植入物（例如，用于髋部和膝部）。除塑料和金属外，陶瓷，陶瓷金属杂化材料和各种复合材料也是众所周知且广泛使用的原材料。

增材制造现在用于几个新兴领域，其中一些需要新材料。在增材制造安全方面具有重要意义的三个重要领域是电子，生物组织和食品（食品和药品）。

虽然这个概念可以追溯到 2004 年[47,58]，但电子电路的 3D 打印仍然是一个活跃的研究领域。然而，此时，使用增材制造技术来生产功能电子设备，如高速计算单元，传感器和无线通信组件，还处于起步阶段[80]。2015 年，Voxel8[74] 发布了第一台支持电子电路印刷的商用 3D 打印机。3D 打印机采用双材料系统，可挤出塑料和导电材料银墨，使电路打印和电子元件集成。可以停止打印机以安装通过传统方式生产的电子元件。这消除了许多困扰直接电路印刷的限制。

活组织的印刷有可能成为一种变革性技术。虽然预计身体部位和整个内脏器官的印刷将成为现实[80]，但仍有许多工作要做。重要的是要注意，在生物组织中，不同类型的细胞经常被组织在独特的分层结构和子结构（也称为体系结构）中。细胞及其空间组织对组织的生物学功能至关重要。尽管如此，这个领域正在迅速发展，并出现了几个应用领域。

像欧莱雅这样的化妆品公司已经使用人类表皮（即皮肤片）多年来测试新产品[15]。人类表皮目前在体内或由外部实体如 Episkin[22] 生长，但该过程很快就

会被 3D 生物印刷取代。另一家公司，TeVido Biodevices[71,80]，已宣布计划使用接受者自己的细胞打印用于乳腺癌重建的皮肤和脂肪移植物。同时,Organovo[57] 提供用于药物发现的定制 3D 打印组织，从而实现药物毒性和在临床前试验中研究的功效。事实上，Organovo 提供“完全人体，结构正确，功能齐全的 3D 组织”，可以构建“几乎任何组织类型，几乎任何疾病。”其产品之一是活肝组织。

另一个新兴的增材制造领域是食品和药品印刷。此时，食品印刷是相当基本的 - 它仅限于一些可以根据需要混合和“烹饪”的成分。目前的食品打印机使用预先填充有成分的容器或具有可再填充的容器，由 3D 打印机的所有者补充新鲜成分[54]。食品印刷的一个优点是生产健康膳食[45]。美国宇航局[51] 认为，太空食品印刷将满足宇航员的营养需求，同时提供更多种类的食物，特别是在长期太空任务中。

2015 年 8 月，Aprecia Pharmaceuticals 宣布美国食品和药物管理局（FDA）批准了第一种 3D 打印药品[33] 。预计药物印刷将使具有成本效益的个性化医疗成为可能。靠近患者的 3D 打印将实现定制生产（针对特定个体的药物化合物，剂量和缓冲剂）和新鲜药物的递送[75] 。为了使这种类型的生产达到主流，3D 打印机必须适应各种药物化合物的操作。

第 5 章　分类

本节描述了对增材制造设备的攻击的语义方面的维度。接下来，介绍以下维度的分类：（i）增材制造工作流程中的受到控制的元素;（ii）操纵这些要素;（iii）交叠着将 3D 打印机作为武器的对抗目标的操纵的影响子集。

5.1.攻击或使用 3D 打印机

图 5.1 概述了如何执行对 3D 打印机的攻击。可以使用各种攻击向量来破坏第 3.1 节中描述的增材制造工作流程的元素。受损组件，它们在工作流中的角色以及攻击者可以控制组件的程度决定了攻击者可以执行的操作。结合增材制造设备的类型，源材料和制造部件的应用，操作决定可实现的效果。

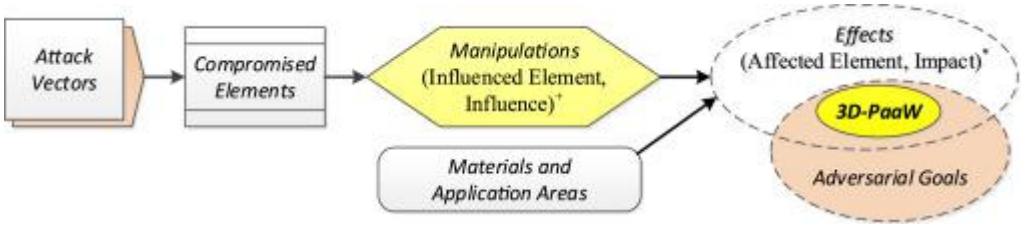

图 5.1 攻击或使用 3D 打印机

根据 Yampolskiy 等人的说法。[85,86]，每个操纵都可以被指定为受影响元素（即操纵物体）和影响（即，行使变化）的一个或多个元组。同样，效果可以指定为受影响元素和影响的元组。Yampolskiy 等。[85,86]认为操纵是一种原因（一种或多种效应）。该命名使得能够无缝描述效果传播因果链。本文强调初始操作。

只有一小部分可以产生的效果与对抗性目标相交叉。此外，只有一小部分交叉点会造成通常与武器相关的伤害。小子集中的效果是对手在试图滥用 3D 打印机作为武器（3D-PaaW）时所寻求的。

3D 打印机的武器化意味着它可以用来造成与武器相关的伤害。常规武器造成动能损害，造成物理破坏，伤害和死亡。核武器，生物武器和化学武器（NBC）通常被认为是非常规武器； 这些武器污染环境，造成健康问题和死亡。武器库中最新增加的是网络武器。正如 Stuxnet 攻击[25]和 Aurora 实验[69]所证明的那样，网络武器可能对基础设施造成物理破坏，甚至可能导致伤亡。

本文考虑了增材制造设备或制造物体可能导致上述类型损坏之一的情况。电子战系统在本文中不被视为武器； 因此，不讨论电子战。然而，滥用 3D 打印机产生电子战效果的可能性不容忽视。

本文不详细讨论攻击向量。这是因为攻击向量与其他类别的网络物理系统的攻击向量基本相同； 这些在研究文献中被广泛涉及。用于在各种应用领域中制造零件的增材制造中使用的材料是众所周知的，并在第 4 节中概述。

本节的其余部分重点介绍了对增材制造安全至关重要的方面：（i）增材制造工作流程中可能受到损害的要素； （ii）可由这些要素进行的操纵； （iii）武器化 3D 打印机的可能性。下面介绍针对 3D 打印机的攻击的所有这些方面（或维度）的分类法。

5.2.受损的元素

针对可能受损的增材制造工作流程中的元素提出以下分类：

（1）演员：可以假设工作流程中的任何参与者都可能是恶意的，任何其他参与者都可能是受害者。因此，来自演员的任何传出边缘都可能是恶意的，并且演员的任何传入边缘都可能产生负面影响。这意味着任何软件更新，替换组件（例如，硬件或机械部件），STL / AMF 文件或源材料都可以由恶意行为者特制。

此外，外部攻击者可能会尝试模拟对工作流具有类似影响的合法参与者。此外，由于增材制造工作流程中的每个参与者都代表一个组织（公司或机构），恶意员工可以以一种使其看起来像恶意的方式规避行动者的内部流程。

（2）软件，硬件和固件：几十年来网络安全的妥协表明，计算系统工作流程中的软件，硬件和固件 - 以及增材制造工作流程中的扩展 - 可以成为攻击者的成功目标。事实证明，社交工程是说服合法用户安装恶意软件或固件的有效攻击媒介。缓冲区溢出攻击及其变体“返回 libc”和面向返回的编程[13,63]仍然是最有效的攻击向量，通过精心设计的输入实现代码注入软件和固件。Stuxnet [25] 已经证明恶意软件正在运行在控制计算机上可以在系统上安装恶意固件，反之亦然。此外，硬件特洛伊木马可以嵌入到设备中； 这些特洛伊木马可以有复杂的激活触发器 [59]来逃避功能测试期间的过早检测。[1]中描述的旁道方法在检测特洛伊木马的能力方面受到限制。

（3）网络通信：网络通信渠道可以通过多种方式受到损害，详见网络安全文献。例如，在控制器计算机上运行的恶意软件（参见图 3.1）可以安装网络过滤器并获得对所有传入和传出数据包的访问。防火墙和网络监控工具广泛使用这种方法，但它经常被恶意软件滥用。

（4）物理供应链：增材制造工作流程涉及各种物理组件的交付。这些包括替换组件（电子和机械），生产和后期制作中使用的各种材料（源材料和支撑结构材料）和制造的 3D 零件。物理供应链明确涵盖了物理组件的运输和存储，提供了无数的妥协机会。除了明显的方法之外，甚至环境参数也会带来危险 - 尤其是储存和运输过程中的温度和湿度，以及运输过程中的振动。

5.3. 操纵

增材制造工作流程的受损元素可用于实施攻击。行使操纵的能力取决于受损元素的类别，其在增材制造工作流程中的角色（或位置）以及对手对受损元素的控制程度。为简单起见，假设对手可以对受损元素进行完全控制。

图 5.2 显示了受损元素类别之间的相关性（与它们在增材制造工作流程中的位置无关）和元素能够行使的操作。操纵被表示为（受影响的元素，影响）的一个或多个元组。因此，提出了两级分类。顶级分类指定受影响元素的类别。相关影响的分类表示为受影响元素的子分类。

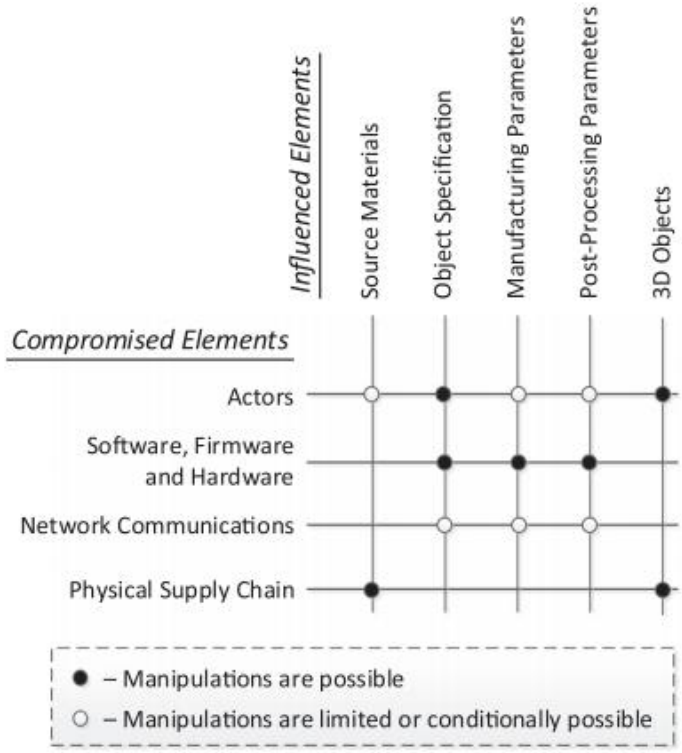

图 5.2 受损的元素和操纵

建议采用以下分类法进行操作：

（1）源材料：操纵源材料的能力是一个标志性方面，它将增材制造系统的安全性与其他网络物理系统的安全性区分开来。源材料不仅指用于制造 3D 物体的材料，还指生产过程中使用的所有其他材料，包括用于支撑结构的材料和使用激光作为热源时的惰性气体（氩气）（真空是当电子需要时梁用作热源）。源材料可

以由生产和/或供应材料的恶意行为者操纵，或者由已经损害供应链的外部对手操纵。虽然恶意生产者或供应商只能操纵他们自己的源材料，但成功瞄准物理供应链的对手可能会破坏任何和所有源材料。在这两种情况下，都可以操作以下源材质属性：

1）材料：材料的修改或替换是一个关键的操作。例如，具有不同机械性能的金属或合金可以与源粉末混合或者可以代替源粉末，或者具有不同导热性的材料可以代替支撑材料。除了直接操纵材料外，间接操作也是可能的。如果在储存或运输过程中操纵温度或湿度等属性，则可以修改源材料属性。对于人体组织和食品和药物印刷中使用的源材料尤其如此。

2）几何形状：在线材形式的源材料的情况下，几何形状的操纵仅限于线材直径。在粉末的情况下，可以在不改变源材料的化学组成的情况下改变粒度，形状因子和规则性。

3）核/生物/化学污染：一种特殊的源材料操纵是其受到危险的核，生物或化学材料的污染。

4）爆炸物：另一种特殊的源材料操作是与易燃或易爆材料的混合物。

请注意，重点不在于增材制造设备（如电路板，电机和机械部件）的改变部件的物理供应。这是一种攻击向量，可用于危害增材制造设备的众多元素。

（2）物体规范：物体规范通常涉及物体的 3D 几何体的描述。如上所述，3D 几何结构通常使用 STL 或 AMF 格式指定。但是，物体规范还可以包括机械特性，尤其是当部件用于安全关键系统时。由于 STL 和 AMF 文件不支持对此类信息的描述，因此通常在补充文档中提供（例如，以 PDF 文件的形式）。物体规范的操作有各种起源和动机：

1）漏洞利用：恶意行为者可以制作物体规范，以便在 3D 打印机制造商的网站上破坏设备。网络折衷可以用于这种操作。众所周知，特制的 PDF 文件可以利用 Adobe Acrobat 和 Adobe Reader 的漏洞[49];这些文件可用于危害用于控制的个

人计算机。STL 和 AMF 文件尚未精心设计，无法将代码注入软件或固件，但这种妥协是一种独特的可能性。

2）不符合：3D 物体与原始规范的偏差或不符合包括打印期间的 3D 几何，尺寸和物体方向。由于增材制造产生的物体的各向异性，取向很重要[2]。受到网络通信危害的对手可以在传输过程中操纵 STL 或 AMF 文件。在控制器计算机上运行的恶意软件可能会向 3D 打印机发送错误或修改的控制命令。3D 打印机中的恶意固件或硬件可以在执行之前更改合法命令，或者只是忽略它们并根据攻击者提供的规范执行命令。

操纵程度可能取决于增材制造工作流程的恶意或受损元素。恶意软件，固件和硬件可以执行任意修改。然而，网络通信通常通过加密隐私和/或消息认证码来保护完整性。因此，只有当它们不受保护或者保护机制具有可被利用的缺陷时，通过受损网络通信对物体规范的操纵才是可行的。

（3）制造参数：ASTM 定义的七种增材制造工艺在源材料的沉积和熔合方式上有所不同。这不可避免地决定了可以操纵的制造参数。对该主题的完整讨论超出了本文的范围。然而，粉末床熔合中的一些关键制造参数包括粉末层的厚度，热源的能量和熔化模式。在 [87] 中讨论了可以在涉及金属和合金的增材制造工艺中操纵的安全相关制造参数。无论制造参数如何，以下两类操作仅基于其范围：

1）不合格：3D 物体的几何精度及其机械性能取决于众多制造参数[28,78]。如果至少一个参数在产生具有所需特性的 3D 物体所需的范围之外，则制造参数的组合被分类为不合格。

2）超出操作范围：每个系统都旨在支持特定操作范围内的参数修改。这同样适用于 3D 打印机。如果至少一个参数在设计 3D 打印机的范围之外，则制造参数的组合被分类为在操作范围之外。

通常，不合格与增材制造设备支持的操作范围无关。可以通过受损软件，固件，硬件或网络通信来操纵若干制造参数。然而，尽管所有这些受损元素都可以轻松实现不符合，但是通过受损网络通信或在控制器计算机上运行的软件进行的第二类操作只能有条件地实现。原因是不妥协的固件或硬件可能会实施安全检查，以防止在支持的参数范围之外的操作。同样，恶意参与者可能受到固件或硬件检查以及他们自己的技能限制。此外，在内部威胁的情况下，物理和网络访问控制可以限制内部人员可能意外或故意执行的操作。

（4）后处理参数：类似的考虑适用于后处理。在热等静压金属部件的情况下，操作可涉及加工的温度和时间以及炉温。再一次，存在相同的两类操作：

1）不合格：至少有一个后处理参数超出了达到所需零件质量所需的范围； 但是，没有一个参数超出设备支持的操作范围。

2）超出操作范围：至少一个后处理参数超出了后处理设备的设计范围。

在这种情况下，受损的固件或硬件可以具有不受限制的操作功能。受损软件或网络通信的操作可能受到固件或硬件中集成的安全和安全机制的限制。相同的机制也会限制恶意行为者的操纵。物理和网络访问控制措施将进一步限制内部人员意外或恶意执行的操纵。

（5）3D 物体：在生产和最终交付之间可以对 3D 物体进行大量操作。这些操作有点类似于在源材料上执行的操作。只有在供应链的相应部分受到损害时才能进行操作。以下类别的操作是可能的：

1）物理损坏：制造的物体在物理上受损。另外，如在源材料的操纵的情况下，在组织和食品和药物印刷的情况下，通过操纵环境控制（例如，运输期间的温度）的间接损害可以是非常有效的。

2）核/生物/化学污染：可能使用危险的核，生物或化学材料污染制成品。

5.4.3D 打印机作为武器

操纵和对抗目标的影响都是多方面的，对于这两组的交集也是如此。本节重点介绍此交叉点的一个子集 - 将 3D 打印机误用为武器（3D-PaaW）的能力。如第 5.1 节所述，这意味着发生物理损害，或者生理和生命受到物理（动能）攻击，核，生物或化学污染或网络攻击的威胁。

这类攻击对民族国家的对手和恐怖组织尤其具有吸引力。然而，该类别对犯罪组织，骇客组织，竞争者和心怀不满的个人也具有吸引力。

针对 3D 打印机提出了两级分类作为武器攻击。顶级类别指定受攻击立即影响的目标。子类别描述了对此目标的影响类型。提出以下分类：

(1)3D 物体：制造物体的属性以使其受到伤害的方式进行更改。损坏取决于物体的更改方式和应用程序。基于所使用的源材料，操纵类别和 3D 物体的应用区域，识别以下子类别：

1)物理特性：可以改变制造物体的物理特性（例如，机械或生物）。任何讨论的操作都可能对物理特性产生影响。物理性质改变的方式取决于许多因素，

包括应用领域，原料和增材制造工艺。例如，改变粉末床熔合工艺中的熔化模式可以影响金属部件的机械性能，并且改变细胞的 3D 放置可以影响印刷组织的生物学性质。

2)核/生物/化学污染：物体在生产期间或之后可能受到污染。源材料的污染可能并不总是有效的。例如，挥发性化学品或生物材料不太可能在粉末床熔合过程中的高温下存活。

3)电子电路：在制造物体中印刷或压印电子器件的能力开启了改变 3D 打印电子电路的可能性。特别是，改变物体规范会打开各种各样的攻击，利用制造物体中受损的电子设备。这包括结合硬件特洛伊木马和侧面信道泄漏信息。请注意，物体规范的更改可以通过更改 STL 或 AMF 文件或由恶意软件，固件或硬件特洛伊木马“在运行中”来提前执行（请参阅第 5.3 节中的相关讨论））。源材料和制造参数的操作对电子器件的影响有限，例如负面影响性能和增加侧通道泄漏。此外，与物体规范的操纵不同，源材料的操纵或制造过程不能完全控制对 3D 打印的电子组件的影响。

(2)3D 打印机：在关键基础设施的背景下，主要关注的是通过操纵来自网络域的控制参数来对基础设施造成物理损害的能力。Stuxnet [25]和 Aurora 实验[69]说明了这种担忧的合法性。显然，为基础设施资产创建零件的增材制造设备本身就是一个有吸引力的目标。这些攻击会产生以下类别的影响：

1)缩短使用寿命：对制造参数的修改会增加增材制造设备部件的磨损，从而缩短设备的使用寿命。受影响的设备组件包括电机以及由电机移动的机械部件。对后处理参数的操纵可以产生类似的效果。例如，在热等静压过程中对压力和温度的操纵可以减少该过程使用的高压容器的寿命。源材料的操作（例如，将源材料与溶剂或易燃材料混合）也会增加设备磨损。

2)无法弥补的损坏：在减少寿命的类别中，增材制造设备的某些部件被损坏。然而，在许多情况下，识别和更换受损部件所涉及的成本可能使设备维修在经济上不可行。当存在重复和/或多个组件故障时也会发生这种情况。

另外，在制造过程或后处理期间的操作会使增材制造设备受到不可修复的损坏。在使用金属的 3D 打印机的情况下，激光或电子束瞄准系统的操纵可导致源材料的不可控制的流动和对容纳室的损坏，导致不可修复的设备损坏。通过操纵源材料可以实现类似的效果。在粉末床熔合的情况下，如果源材料被具有较低熔点的

材料替换，则所产生的不可控制的流动会不可挽回地损坏设备。物体规范的操作也可以具有类似的效果。然而，

3)爆炸/内爆：在源材料中混合高度易燃或易爆的材料可能会在制造过程中导致爆炸。通过操纵制造和后处理参数可以实现类似的效果。当电子束用作热源时需要高真空[3] ； 否则电子束偏转并且不会聚焦在该部分上。如果调整制造参数以将光束聚焦在诸如容纳室之类的其他位置上，则对腔室的损坏可能导致内爆。

激光可以在正常的大气环境中有效地工作。然而，惰性气体（通常是氩气）被引入容纳室中，因为金属粉末（例如，钛和铝合金）通常是可燃的。如果收容室受损并且金属粉末暴露在大气中，可能会发生火灾或粉尘爆炸[55,56]。

(3)环境：最后，增材制造环境（例如，建筑物）可能成为 3D 打印机的目标，作为武器攻击。可能存在以下类别的影响：

1)爆炸/爆炸：爆炸或内爆可能会损坏增材制造设备及其周围环境，包括装有设备的建筑物。在粉末床熔合过程的情况下，爆炸或内爆可以将可燃粉末释放到环境中。由于分散的可燃粉尘的数量和浓度增加，二次爆炸可能比一次爆炸更具破坏性[55]。这可能导致伤害，死亡和制造设施的破坏[55]。

2)火灾：火灾是爆炸或内爆的常见次要影响。火灾的程度取决于爆炸或内爆附近是否存在易燃材料。操作源材料或制造参数可能导致火灾而不会发生爆炸或内爆。例如，用易燃材料替换用于印刷的塑料细丝可能导致火灾。

3)核/生物/化学污染：显然，如果源材料或制造的 3D 物体受到污染，其直接环境也会受到污染，并且这些环境中的人员会接触到有害物质。增材制造过程的操作也可以将细粉末释放到环境中。根据化学成分和颗粒大小，释放的粉末可归类为有害物质。

请注意，3D 打印机中未提及对增材制造设备及其环境的网络攻击作为武器分类。虽然这些攻击是可能的，但实际上很可能，它们被认为是用于损害增材制造工作流程的各种元素的载体（参见图 5.1）。

此外，仅考虑对增材制造设备进行单独的不协调攻击。可以想象，协同攻击可能会导致 3D 打印机作为武器类别的其他影响。例如，多个 3D 打印机的协同攻击可能产生可能导致电力中断的电涌。

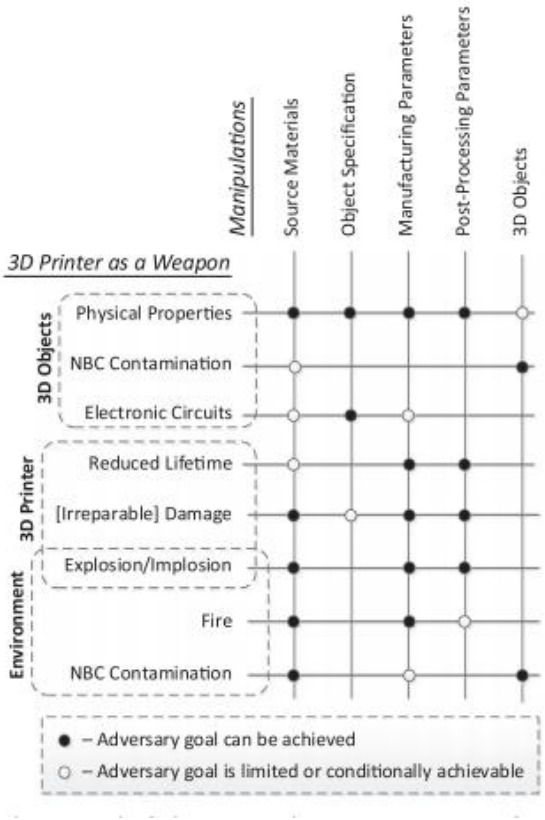

图 5.3 操纵和 3D 打印机作为武器攻击

图 5.3 总结了 3D 打印机作为上面讨论的武器攻击。显然，这些攻击会导致安全违规并产生许多次要影响，包括在物理，环境，社会经济和地缘政治领域可能产生的影响。

第 6 章　3D 打印机作为武器的特点

不同的武器类型具有不同的属性。对于自动化武器，属性包括精度和射击率；　对于制导炸弹，其性能包括精度，穿透深度和爆炸半径。3D 打印机的武器化需要类似的特性。

以下分类法（图 6.1 中总结）被提议用于 3D 打印机作为武器：

（1）定位精度：精确度是武器的重要特征。它指定与所需目标的偏差。

1）3D 物体：操作 3D 物体时可以实现高目标精度。当恶意软件，固件或硬件进行操作时，可以识别目标 3D 物体的唯一蓝图，并将其用作攻击的触发器。然而，在核，生物或化学污染的情况下，目标精确度取决于源材料或制造物体是否已被污染。在前一种情况下，精度相当低，仅限于原材料制造商或供应链妥协的演员。在后一种情况下，精度非常高，因为可以针对为特定客户创建的单个制造零件。

2）3D 打印机：当针对增材制造设备时，可达到的精度是中等的。可以实现对制造商现场的关注，但几乎不可能区分出向不同客户的相同增材制造系统。

3）环境：精确瞄准增材制造环境的能力相当低。这是因为对手无法控制环境，包括其随时间的变化以及特定时间在特定位置的人员的存在。

（2）影响范围：另一个重要特征是攻击能够影响广泛的区域。

1）3D 物体：当制造功能部件被操纵时，冲击区域非常大。这是因为这些部件将被用作关键基础设施中众多可能对安全至关重要的系统和设备中的功能组件。

2）3D 打印机：当针对增材制造设备时，影响区域很小，因为它局限于单件设备。唯一的例外是爆炸或内爆，这也可能影响周围的环境。

3）环境：对环境的攻击会产生中等影响。影响将仅限于制造场所，最多只限于其邻近区域。

（3）附带损害：附带损害是武器的重要财产。它衡量武器对非预期目标（系统，人类和环境）的影响程度。

1）3D 物体：操纵制造的 3D 物体产生的附带损害取决于操纵的类型。当操纵电子电路时，可以控制执行攻击的条件（例如，通过引入复杂的触发器）。

当操纵物理（例如，机械）属性或 3D 物体被污染时，附带损害可以扩展到使用制造物体的任何系统或个人以及使用物体的环境。

2）3D 打印机：当增材制造设备成为目标时，附带损害相当低，因为受损设备包含损坏。但是，在爆炸或内爆的情况下，直接环境也可能受到影响。

3）环境：火灾和污染会产生中等程度的附带损害。损害将仅限于制造场地，最多只能在其附近。

（4）隐身：如果没有立即检测到武器或者其效果不一定归因于武器，则该武器是隐身的。

1）3D 物体：对制造物体的物理属性的操纵可能在很长一段时间内未被检测到。然而，在飞机坠毁的情况下，通常的做法是将特定类型的飞机接地并对事故及其原因进行彻底调查。这样的调查可能会发现物体的物理属性被修改。因此，操纵的隐秘程度将是中等的。核，生物或化学污染的隐形水平甚至更低，因为它们更容易被发现。然而，电子设备的修改可能会在很长一段时间内未被发现，直到设备被触发并且事件被调查。

2）3D 打印机：正如 Stuxnet 所示，设备寿命和损坏的减少可能无法检测到或长时间归因于其他原因。然而，在注意到反复出现的问题之后，彻底的调查最终会发现攻击。爆炸或内爆会立即引发全面调查。

3）环境：几乎可以立即检测到火灾，如爆炸或内爆。因此，攻击的隐秘程度会很低。然而，环境污染的检测将取决于安装在制造现场的传感器。如果没有安装某些类型污染的传感器，那么攻击可能会被发现，直到健康问题或其他一些异常引发调查。

（5）攻击重复性：武器的特点还在于它可以多次使用。

1）3D 物体：显然，可以为许多生产的零件复制对 3D 物体的攻击。

2）3D 打印机：假设受攻击的元素没有被攻击本身损坏，可以反复重复减少设备寿命或造成设备损坏的攻击。但是，攻击仅限于设备使用期间。对增材制造设备造成爆炸或内爆或其他一些不可挽回的损害的攻击将是一次性攻击。

3）环境：除非火灾不可挽回地损害增材制造设备或发现引起火灾的攻击，否则攻击将是可重复的。对于污染环境的攻击也是如此。

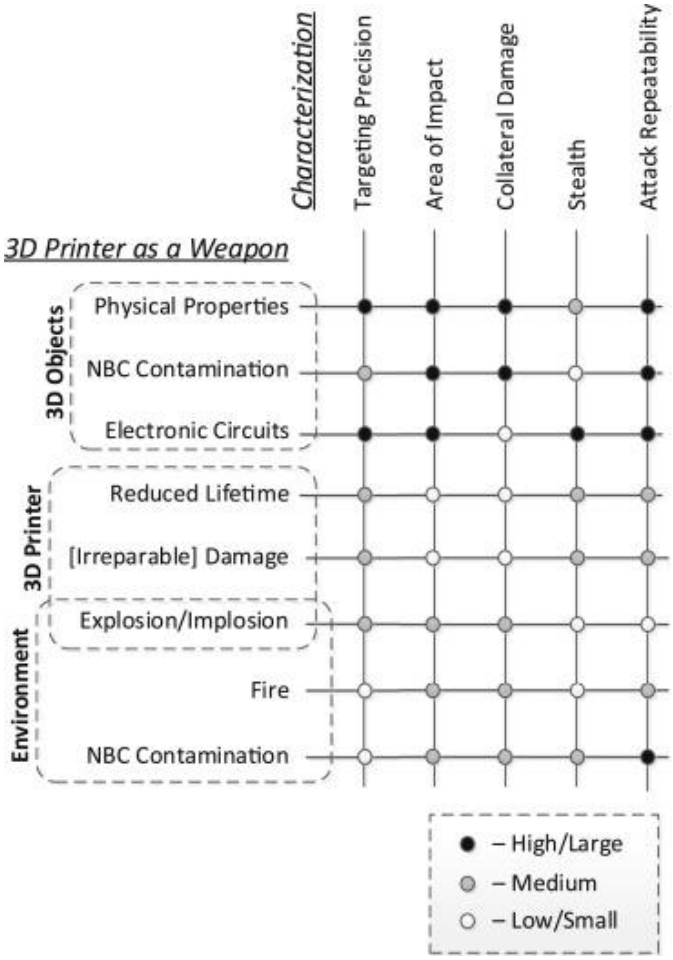

图 6.1 以 3D 打印机作武器的特色

请注意，只考虑了对增材制造设备的单独未协调攻击。在协同攻击的情况下，3D 打印机作为武器攻击类别及其特征将需要扩展来解释多次攻击以及进行攻击所涉及的协调。

第 7 章　结论

增材制造或 3D 打印是一项变革性技术,将在关键制造领域发挥重要作用。然而，巨大的市场潜力,以及增材制造的经济，地缘政治和其他影响，将不可避免地引起一些敌对分子的注意，包括从个人到国家决策者。

本文描绘了可能产生物理影响的 3D 打印机或 3D 打印机的攻击情况。由于这些攻击可能造成物理伤害以及伤害和死亡,因此它们被称为使用 3D 打印机作为武器的攻击。增材制造工作流程中容易受损的的元素已经由分类法所指定,对于受损元件的操作是可以实现的并且可用于 3D 打印机作为攻击武器子集驻留在交叉点的通过可实现对抗的目标和效果操作。另外，已经详细描述了作为武器攻击的 3D 打印机的许多可能示例。

本文中提出的攻击主要是假设的，其有效性需要实验确认或来自现实世界的报告。无论如何，鉴于巨大的伤害潜力，必须对假设和真实的 3D 打印机作为武器攻击进行编目和分析，以更好地了解其性质和范围。

希望本文中提出的分类法将激发对增材制造安全性方面的认真研究。增材制造是一种很有前景但非常危险的技术。研究机构和供应商社区必须更加关注防御战略和机制的发展,以减轻 3D 打印机用作武器时可能产生的严重影响。

请注意，本文中表达的观点和结论是作者的观点和结论。它们不一定代表 BICES 集团执行官或其成员的意见或立场。

参考文献

[1] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi and B. Sunar, Trojan detection using IC fingerprinting, *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 296–310, 2007.

[2] S. Ahn, M. Montero, D. Odell, S. Roundy and P. Wright, Anisotropic material properties of fused deposition modeling ABS, *Rapid Prototyping Journal*, vol. 8(4), pp. 248–257, 2002.

[3] Arcam, Electron Beam Melting – in the Forefront of Additive Manufacturing, Molndal, Sweden (arcam.com/technology/electron-beam-melting), 2014.

[4] A. Avizienis, J. Laprie, B. Randell and C. Landwehr, Basic concepts and taxonomy of dependable and secure computing, *IEEE Transactions on Dependable and Secure Computing*, vol. 1(1), pp. 11–33, 2004.

[5] A. Bagsik, V. Schoppner and E. Klemp, FDM part quality manufactured with Ultem*9085, *Proceedings of the Fourteenth International Scientific Conference on Polymeric Materials*, 2010.

[6] B. Berman, 3-D printing: The new industrial revolution, *Business Horizons*, vol. 55(2), pp. 155–162, 2012.

[7] S. Bradshaw, A. Bowyer and P. Haufe, The intellectual property implications of low-cost 3D printing, *ScriptEd*, vol. 7(1), pp. 5–31, 2010.

[8] E. Byres and J. Lowe, The myths and facts behind cyber security risks for industrial control systems, *Proceedings of the VDE Kongress*, 2004.

[9] T. Campbell and O. Ivanova, Additive manufacturing as a disruptive technology: Implications of three-dimensional printing, *Technology and Innovation*, vol. 15, pp. 67–79, 2013.

[10] T. Campbell, C. Williams, O. Ivanova and B. Garrett, Could 3D Printing Change the World? Technologies, Potential and Implications of Additive Manufacturing, Atlantic Council, Washington, DC, 2011.
[11] A. Chakrabarti and G. Manimaran, Internet infrastructure security: A taxonomy, *IEEE Network*, vol. 16(6), pp. 13–21, 2002.
[12] K. Chan, M. Koike, R. Mason and T. Okabe, Fatigue life of titanium alloys fabricated by additive layer manufacturing techniques for dental implants, *Metallurgical and Materials Transactions A*, vol. 44(2), pp. 1010–1022, 2013.
[13] S. Checkoway, L. Davi, A. Dmitrienko, A. Sadeghi, H. Shacham and M. Winandy, Return-oriented programming without returns, *Proceedings of the Seventeenth ACM Conference on Computer and Communications Security*, pp. 559–572, 2010.
[14] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner and T. Kohno, Comprehensive experimental analyses of automotive attack surfaces, *Proceedings of the Twentieth USENIX Conference on Security*, 2011.
[15] K. Collins, L'Oreal is 3D printing its own human skin to test cosmetics, *Wired*, May 19, 2015.
[16] Cornell Creative Machines Lab, Standard Specification for Additive Manufacturing File Format (Draft F XXXX-10), Cornell University, Ithaca, New York (creativemachines.cornell.edu/sites/default/files/AMF_V0.47.pdf), 2014.
[17] S. Dadbakhsh and L. Hao, Effect of layer thickness in selective laser melting on microstructure of Al/5 wt.%Fe_2O_3 powder consolidated parts, *Scientific World Journal*, vol. 2014, article id. 106129, 2014.
[18] K. Dempsey and C. Paulsen, Risk Management for Replication Devices, NISTIR 8023, National Institute of Standards and Technology, Gaithersburg, Maryland, 2015.
[19] DUS Architects, 3D PRINT Architecture, Amsterdam, The Netherlands (www.dusarchitects.com), 2014.
[20] S. East, J. Butts, M. Papa and S. Shenoi, A taxonomy of attacks on the DNP3 protocol, in *Critical Infrastructure Protection III*, C. Palmer and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 67–81, 2009.
[21] Electronic Industries Association, Interchangeable Variable Block Data Format for Positioning, Contouring and Contouring/Positioning Numerically Controlled Machines, EIA Standard RS-274-D, Washington, DC, 1980.
[22] Episkin, RHE SkinEthic, Lyon, France (www.episkin.com/RHE.asp), 2015.
[23] ESET, ACAD/Medre.A, 10000's of AutoCAD Designs Leaked in Suspected Industrial Espionage, San Diego, California (www.welivesecurity.com/media_files/white-papers/ESET_ACAD_Medre_A_whitepaper.pdf), 2015.
[24] European Powder Metallurgy Association, Additive Manufacturing Technology, Shrewsbury, United Kingdom (epma.com/additive-manufacturing-technology), 2014.
[25] N. Falliere, L. O'Murchu and E. Chien, W32.Stuxnet Dossier, Version 1.4, Symantec, Mountain View, California, 2011.
[26] L. Forbes, H. Vu, B. Udrea, H. Hagar, X. Koutsoukos and M. Yampolskiy, SecureCPS: Defending a nanosatellite cyber-physical system, *Proceedings of the SPIE*, vol. 9085, 2014.
[27] J. Foust, SpaceX unveils its "21st century spaceship," *NewSpace Journal* (www.newspacejournal.com/2014/05/30/spacex-unveils-its-21st-century-spaceship), May 30, 2014.
[28] W. Frazier, Metal additive manufacturing: A review, *Journal of Materials Engineering and Performance*, vol. 23(6), pp. 1917–1928, 2014.
[29] General Electric, Hardware meets software in advanced manufacturing, Fairfield, Connecticut (www.ge.com/stories/hardware-meets-software-advancedmanufacturing), 2015.
[30] I. Gibson, D. Rosen and B. Stucker, *Additive Manufacturing Technologies: Rapid Prototyping to Direct Digital Manufacturing*, Springer, New York, 2010.
[31] S. Hansman and R. Hunt, A taxonomy of network and computer attacks, *Computers and Security*, vol. 24(1), pp. 31–43, 2005.
[32] D. Helbing, Globally networked risks and how to respond, *Nature*, vol. 497(7447), pp. 51–59, 2013.
[33] J. Hicks, FDA approved 3D printed drug available in the US, *Forbes*, March 22, 2016.
[34] J. Hiller and H. Lipson, STL 2.0: A proposal for a universal multi-material additive manufacturing file format, *Proceedings of the Solid Freeform Fabrication Symposium*, pp. 266–278, 2009.
[35] S. Huang, P. Liu, A. Mokasdar and L. Hou, Additive manufacturing and its societal impact: A literature review, *International Journal of Advanced Manufacturing Technology*, vol. 67 (5–8), pp. 1191–1203, 2013.
[36] P. Huitsing, R. Chandia, M. Papa and S. Shenoi, Attack taxonomies for the Modbus protocols, *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 37–44, 2008.
[37] S. Kelly and S. Kampe, Microstructural evolution in laser-deposited multilayer Ti-6Al-4V builds: Part I; Microstructural characterization, *Metallurgical and Materials Transactions A*, vol. 35(6), pp. 1861–1867, 2004.
[38] S. Kelly and S. Kampe, Microstructural evolution in laser-deposited multilayer Ti-6Al-4 V builds: Part II; Thermal modeling, *Metallurgical and Materials Transactions A*, vol. 35(6), pp. 1869–1879, 2004.
[39] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage, Experimental security analysis of a modern automobile, *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 447–462, 2010.
[40] T. Krol, M. Zah and C. Seidel, Optimization of supports in metal-based additive manufacturing by means of finite element models, *Proceedings of the International Solid Freeform Fabrication Symposium*, 2012.
[41] M. Krotofil, A. Cardenas, J. Larsen and D. Gollmann, Vulnerabilities of cyber-physical systems to stale data – Determining the optimal time to launch attacks, *International Journal of Critical Infrastructure Protection*, vol. 7(4), pp. 213–232, 2014.
[42] J. Laprie, Dependable computing and fault-tolerance: Concepts and terminology, *Proceedings of the Fifteenth International Symposium on Fault Tolerant Computing*, pp. 2–11, 1985.
[43] H. Lipson, AMF tutorial: The basics (Part 1), 3D Printing and Additive Manufacturing, vol. 1(2), pp. 85–87, 2014.
[44] B. Liu, R. Wildman, C. Tuck, I. Ashcroft and R. Hague, Investigation of the effect of particle size distribution on processing parameters optimization in the selective laser melting process, *Proceedings of the International Solid Freeform Fabrication Symposium*, pp. 227–238, 2011.
[45] J. Luimstra, Star Trek inspires Nestle to work on personalized nutrition project, 3DPrinting.com (3dprinting.com/news/star-trek-inspires-nestle-workpersonalized-nutrition-project), June 25, 2014.
[46] B. Macq, P. Alface and M. Montanola, Applicability of watermarking for intellectual property rights protection in a 3D printing scenario, *Proceedings of the Twentieth International Conference on 3D Web Technology*, pp. 89–95, 2015.
[47] E. Malone and H. Lipson, Freeform fabrication of electroactive polymer actuators and electromechanical devices, *Proceedings of the Fifteenth Solid Freeform Fabrication Symposium*, pp. 697–708, 2004.
[48] D. Manfredi, F. Calignano, M. Krishnan, R. Canali, E. Ambrosio and E. Atzeni, From powders to dense metal parts: Characterization of a commercial AlSiMg alloy processed

through direct metal laser sintering, *Materials*, vol. 6(3), pp. 856–869, 2013.
[49] Microsoft, Microsoft Security Intelligence Report, Volume 18, July through Deecember 2014, Redmond, Washington, 2015.
[50] J. Mirkovic and P. Reiher, A taxonomy of DDoS attacks and DDoS defense mechanisms, *ACM SIGCOMM Computer Communication Review*, vol. 34(2), pp. 39–53, 2004.
[51] National Aeronautics and Space Administration, 3D Printing: Food in Space, Washington, DC (www.nasa.gov/directorates/spacetech/home/feature_3d_food.html#.V1IdJpErKhd), 2013.
[52] National Defense Industrial Association, Cybersecurity for Advanced Manufacturing, White Paper, Arlington, Virginia, 2014.
[53] National Institute of Standards and Technology, Measurement Science Roadmap for Metal-Based Additive Manufacturing, Workshop Summary Report, Gaithersburg, Maryland, 2013.
[54] Natural Machines, Foodini – A 3D food printer, Barcelona, Spain (www.naturalmachines.com), 2015.
[55] Occupational Safety and Health Administration, Hazard Alert: Combustible Dust Explosions, OSHA Fact Sheet, DSG 12/2014, Washington, DC (www.osha.gov/OshDoc/data_General_Facts/OSHAcombustibledust.pdf), 2014.
[56] Office of Public Affairs, After explosion, U.S. Department of Labor's OSHA cites 3-D printing firm for exposing workers to combustible metal powder, electrical hazards – Powderpart Inc. faces $64,400 in penalties, OSHA Regional News Release, Department of Labor, Washington, DC, May 20, 2014.
[57] Organovo, Structurally and functionally accurate bioprinted human tissue models, San Diego, California (www.organovo.com), 2015.
[58] D. Periard, E. Malone and H. Lipson, Printing embedded circuits, *Proceedings of the Eighteenth Solid Freeform Fabrication Symposium*, pp. 503–512, 2007.
[59] R. Rad, X. Wang, M. Tehranipoor and J. Plusquellic, Power supply signal calibration techniques for improving detection resolution of hardware Trojans, *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, pp. 632–639, 2008.
[60] G. Ram, Y. Yang and B. Stucker, Effect of process parameters on bond formation during ultrasonic consolidation of aluminum alloy 3003, *Journal of Manufacturing Systems*, vol. 25(3), pp. 221–238, 2006.
[61] S. Ravi, A. Raghunathan, P. Kocher and S. Hattangady, Security in embedded systems: Design challenges, *ACM Transactions on Embedded Computing Systems*, vol. 3(3), pp. 461–491, 2004.
[62] S. Rinaldi, J. Peerenboom and T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems*, vol. 21(6), pp. 11–25, 2001.
[63] R. Roemer, E. Buchanan, H. Shacham and S. Savage, Return-oriented programming: Systems, languages and applications, *ACM Transactions on Information and System Security*, vol. 15(1), article no. 2, 2012.
[64] C. Schade, T. Murphy and C. Walton, Development of Atomized Powders for Additive Manufacturing, Hoeganaes Corporation, Cinnaminson, New Jersey (www.gkn.com/hoeganaes/media/Tech%20Library/Schadeade-Atomized%20Powders%20for%20Additive%20Manufacturing%20(1).pdf), 2014.
[65] Science in Public, The world's first printed jet engine, Melbourne, Australia (www.scienceinpublic.com.au/mediareleases/monash-avalonairshow-2015), February 26, 2015.
[66] J. Slay and M. Miller, Lessons learned from the Maroochy water breach, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 73–82, 2007.
[67] A. Sternstein, Things can go kaboom when a defense contractor's 3-D printer gets hacked, *Nextgov*, September 11, 2014.
[68] L. Sturm, C. Williams, J. Camelio, J. White and R. Parker, Cyber-physical vunerabilities in additive manufacturing systems, *Proceedings of the Twenty-Fifth International Solid Freeform Fabrication Symposium*, 2014.
[69] M. Swearingen, S. Brunasso, J. Weiss and D. Huber, What you need to know (and don't) about the Aurora vulnerability, *POWER Magazine*, September 1, 2013.
[70] A. Tarantola, DARPA to develop best practices for 3D printing, *Engadget* (www.engadget.com/2015/05/31/darpa-to-develop-best-practicesfor-3d-printing), May 31, 2015.
[71] TeVido BioDevices, About Us, Austin, Texas (tevidobiodevices.com/about-us), 2015.
[72] D. Thomas, Economics of the U.S. Additive Manufacturing Industry, NIST Special Publication 1163, National Institute of Standards and Technology, Gaithersburg, Maryland, 2013.
[73] D. Thomas and S. Gilbert, Costs and Cost Effectiveness of Additive Manufacturing, NIST Special Publication 1176, National Institute of Standards and Technology, Gaithersburg, Maryland, 2014.
[74] Voxel8, The world's first 3D electronics printer, Somerville, Massachusetts (www.voxel8.co), 2015.
[75] J. Wakefield, First 3D-printed pill approved by U.S. authorities, *BBC News*, August 4, 2015.
[76] F. Wang, S. Williams, P. Colegrove and A. Antonysamy, Microstructure and mechanical properties of wire and arc additive manufactured Ti-6Al-4V, *Metallurgical and Materials Transactions A*, vol. 44(2), pp. 968–977, 2013.
[77] M. Weinberg, It will be awesome if they don't screw it up: 3D printing, intellectual property and the fight over the next great disruptive technology, Public Knowledge, Washington, DC (www.publicknowledge.org/files/docs/3DPrintingPaperPublicKnowledge.pdf), 2010.
[78] D. Welch and S. Lathrop, Wireless security threat taxonomy, *Proceedings of the IEEE SMC Information Assurance Workshop*, pp. 76–83, 2003.
[79] L. Wells, J. Camelio, C. Williams and J. White, Cyber-physical security challenges in manufacturing systems, *Manufacturing Letters*, vol. 2(2), pp. 74–77, 2014.
[80] Wohlers Associates, Wohlers Report 2015, Fort Collins, Colorado, 2015.
[81] M. Wolf, M. Minzlaff and M. Moser, Information technology security threats to modern e-enabled aircraft: A cautionary note, *Journal of Aerospace Information Systems*, vol. 11(7), pp. 447–457, 2014.
[82] M. Yampolskiy, T. Andel, J. McDonald, W. Glisson and A. Yasinsac, Intellectual property protection in additive layer manufacturing: Requirements for secure outsourcing, *Proceedings of the Fourth Program Protection and Reverse Engineering Workshop*, article no. 7, 2014.
[83] M. Yampolskiy, T. Andel, J. McDonald, W. Glisson and A. Yasinsac, Towards security of additive layer manufacturing, presented at the *Thirtieth Annual Computer Security Applications Conference*, 2014.
[84] M. Yampolskiy, P. Horvath, X. Koutsoukos, Y. Xue and J. Sztipanovits, Systematic analysis of cyber-attacks on the CPS-evaluating applicability of the DFD-based approach, *Proceedings of the Fifth International Symposium on Resilient Control Systems*, pp. 55–62, 2012.
[85] M. Yampolskiy, P. Horvath, X. Koutsoukos, Y. Xue and J. Sztipanovits, Taxonomy for descriptions of cross-domain attacks on CPSs, *Proceedings of the Second ACM International Conference on High Confidence Networked Systems*, pp. 135–142, 2013.
[86] M. Yampolskiy, P. Horvath, X. Koutsoukos, Y. Xue and J. Sztipanovits, A language for describing attacks on cyber-physical systems, *International Journal of Critical Infrastructure Protection*, vol. 8, pp. 40–52, 2015.
[87] 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, Heidelberg, Germany, pp. 169–183, 2015.
[88] B. Zhu, A. Joseph and S. Sastry, A taxonomy of cyber attacks on SCADA systems, *Proceedings of the International Conference on the Internet of Things and the Fourth International Conference on Cyber, Physical and Social Computing*, pp. 380–388, 2011.

致谢