Homeland Security
Science and Technology

Homeland Security Science and Technology Advisory Committee (HSSTAC): Quadrennial Homeland Security Review Subcommittee

Adaptive Manufacturing White Paper

March 10, 2017

Homeland Security

Science and Technology

This publication is presented on behalf of the Homeland Security Science and Technology Advisory Committee, Quadrennial Homeland Security Review Subcommittee, Adaptive Manufacturing, chaired by Byron Collie with contributions from Dr. Gerald Parker, Dr. Yacov Haimes, Mr. Daniel Dubno as part of recommendations to the Department of Homeland Security, Under Secretary for Science and Technology, Robert Griffin (*Acting*).

<Signature on File>

Byron Collie
Technology Fellow & Head of Cyber Intelligence
Goldman Sachs Group

HSSTAC Staff: Michel Kareis, HSSTAC Executive Director/DFO and Gretchen Cullenberg, QHSR Subcommittee support.

Homeland Security
Science and Technology

ADAPTIVE MANUFACTURING AND HOMELAND SECURITY

Mr. Byron Collie, Subcommittee Chair; Dr. Gerald Parker; Dr. Yacov Haimes; and Mr. Daniel Dubno.

White Paper for HSSTAC Quadrennial Homeland Security Review (QHSR) Subcommittee in support of the 2018 QHSR

Introduction and Problem Statement

Advancing digitally enabled, adaptive manufacturing technologies offer the opportunity for a new age in manufacturing with ubiquitous access to rapid prototyping, small scale production, self-assembling structures and a revolution in bioengineering through bioprinting. These systems and capabilities also present substantial risks offer a tempting target for cyber adversaries as well as the direct potential for misuse, through introduction of fatal flaws and vulnerabilities into manufactured items as well as the opportunity for adversaries to use these technologies to create illicit tools and weapons.

The term "Adaptive Manufacturing" is not well defined by any authoritative source so for the purposes of this paper, we will apply a broad definition, similar to NIST's definition of Direct Digital Manufacturing (DDM):

> *Adaptive Manufacturing refers to those technologies that provide the ability to:*
>
> - *Observe, measure, interact and adjust processes in real-time to ensure manufactured components meet precise tolerances and specifications,*
> - *Conduct automated interaction with the end to end supply chain for production of an object, including in the ability for automated raw materials management, quality assurance and similar product lifecycle management,*
> - *Translate digital models into three dimensional solid objects supporting rapid prototyping and creation of components and/or tools without the need to drastically retool (3D printing, also referred to as Additive Manufacturing),*
> - *Translate digital models into three dimensional solid objects composed of smart, self-transforming or self-assembling materials that alter their structure over time or in response to stimuli (4D printing), and*
> - *Translate digital models into organic structures by creating cell patterns in a confined space using 3D printing technologies, where cell function and viability are preserved within the printed construct to form a functioning organic system (Bioprinting). 4D bioprinting is "the printing of smart, environmentally responsive biological structures, tissues and organs. 4D bioprinting begins with the printing of multiple cells or biological*

matrices resulting in structures that undergo subsequent designed and anticipated (not spontaneous) but self-originated development in response to an environment."[1]

These diverse but interrelated technologies provide capabilities which, from the perspective of humanity only a short time ago, are bordering on the realm of the science fiction "replicator." These technologies are enabled by, and depend upon, the increasing capabilities and decreasing cost of advanced digital sensing, processing, data analysis, machine learning and communications integrated into cyber-physical systems (CPS).[2] For the foreseeable future the United States public and private sectors will need to invest in these technologies to provide secure and adaptable production, supply chain management and distribution to achieve manufacturing competitiveness in global markets.

Looking beyond the technology, the World Economic Forum (WEF) has done substantial work through its Global Agenda Council on the Future of Manufacturing to assess the drivers for the next generation of fabrication. Adaptive Manufacturing (referred to as Cyber-Physical Production by WEF) provides an array of new opportunities for factories of the future, such as (i) monitoring production processes remotely; (ii) having production systems adjust automatically based on sensor readings, improved efficiency (e.g. energy usage) or decreased failure output; and (iii) using machines that automatically replenish stocks across the supply chain.[3]

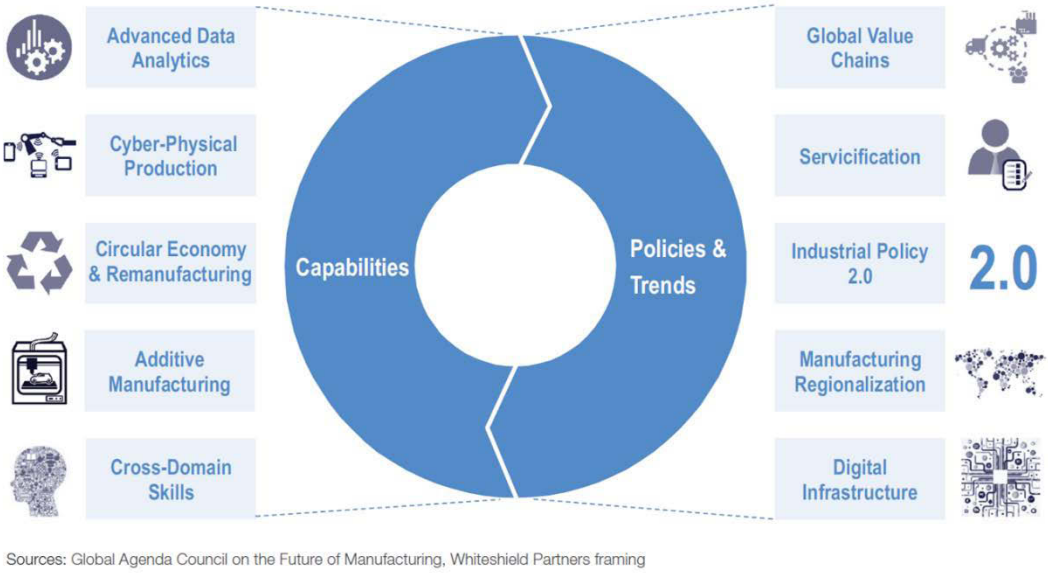

Figure 1 - Drivers of the Future Manufacturing[4]

[1] http://cellculturedish.com/2016/01/another-perspective-on-4d-bioprinting/
[2] https://en.wikipedia.org/wiki/Cyber-physical_system
[3] https://www.weforum.org/reports/future-manufacturing-driving-capabilities-enabling-investments
[4] http://www3.weforum.org/docs/GAC16_The_Future_of_Manufacturing_report.pdf

Manufacturing regionalization shown in the diagram above also highlights the trend to move factories from an "off-shore" model to a "nearshore" model, where manufacturing services are proximate to where demand and innovation take place. One reason for this trend is China's labor rates are increasing at about 20% per year, and rising transportation costs, creating a more favorable environment for North American manufacturers. In addition, weather and natural disasters introduce increasing supply chain risks in Asia for off-shore services. As an example, the 2011 Japanese tsunami significantly disrupted the supply chain throughout the U.S. for major industries including information technology, consumer and industrial electronics and automobiles.[5]

No digital interconnected technology comes, however, without risk of compromise and disruption by human adversaries, with potential for catastrophic consequences to those network-connected cyber-physical systems which may impact security, health and safety. Adaptive manufacturing systems may be targeted by adversaries to steal trade secrets and intellectual property, disrupt or manipulate the manufacturing process and supply chain, including introduction of flaws and malicious logic into manufactured hardware or software. These technologies may also be misused to manufacture contraband items including weapons and other prohibited items outside of established and sometimes monitored channels. There are already examples of the compromise of manufacturing environments resulting in significant damage, as will be described later.

As we look ahead the next four years and beyond, it is an inescapable reality that the digital attack surface of the manufacturing sector will continue to dramatically expand as Adaptive Manufacturing systems are interconnected with networks that have not been architected and hardened sufficiently to deal with the escalating cyber threat environment. These networks will be further interconnected, potentially globally, to support seamless, automated production and supply chain management increasing interdependency and risk.

The evolution of Adaptive Manufacturing technologies will support a continued strong pipeline of innovation in materials, technology and processes. The United States position as a top manufacturing nation will however require continued focus on research and development (R&D) through academic investment, talent development and venture capital investment. The benefits of the technology are expected to drastically increase the market for the technology significantly, from $4.1 billion in 2014 to more than $21 billion globally by 2020.[6]

McKinsey Global Institute's (MGI) 2012 paper "Manufacturing the future: The next era of global growth and innovation"[7] highlights the role of manufacturing in driving innovation and productivity in advanced economies and economic advancement in developing ones. MGI's January 2017 report on "Harnessing automation for a future that works"[8] describes a bright future, heralding a fourth industrial automation

[5] http://www.nytimes.com/2011/03/20/business/20supply.html?pagewanted=all&_r=0
[6] Terry Wohlers, Wohlers report 2015: Additive manufacturing and 3D printing state of the industry, 2015."
[7] http://www.mckinsey.com/business-functions/operations/our-insights/the-future-of-manufacturing
[8] http://www.mckinsey.com/global-themes/digital-disruption/harnessing-automation-for-a-future-that-works

revolution enabled by advanced sensors and increasing cognitive capabilities, where machines will become capable of accomplishing tasks and processes previously thought impossible benefiting an aging global population with increasing wealth and expanding markets for manufactured items.

With respect to sensor driven adaptive technologies, the aerospace industry has been a rapid adopter and innovator to allow manufacture of critical components requiring higher precision and tighter tolerances including jet engine turbine blades, vanes and other components.[9]

Automation of ordering through product delivery and lifecycle management is an area of significant focus and development for many manufacturers and distributers. Robotic Process Automation (RPA) [10] will support integration of automation into existing human driven production and supply chain processes. Price Waterhouse Cooper's estimates that as much as 45% of all human work activities can be automated using RPA agents, driven by Business Process Management logic, with an estimated savings of $2 trillion dollars per annum in wages. Amazon demonstrated its commitment to achieving these objectives at the distribution center level when in 2012 it paid $775 million to acquire Kiva Systems, renamed to Amazon Robotics.[11]

3D printing is not a new technology, celebrating 36 years since it was first proposed by Hideo Kodama of Nagoya Municipal Industrial Research Institute. The revolution in 3D printing that began in the late 2000's will continue to enable and inspire consumers and small companies to rapidly create objects and tools from scratch and at small scales, capabilities which were previously uneconomical and time consuming. The "Maker Movement" is likely to continue to expand as market forces drive increased 3D/4D printing capabilities and materials at lower cost. Gartner predicts that more than 5.6 million 3D printers will be shipped worldwide by 2019.[12] The opportunity for rapid, low cost innovation is not just available to those who can afford a printer though, with many community libraries in the United States making 3D printers free available locally at materials used cost only.

3D printers are not limited to use only in small scale prototyping and development. High-end Fused Deposition Modeling (FDM) based 3D printers are already used in fields including automotive and aerospace manufacture, and in medical devices. The Airbus 350 XWB airliner is currently flying with more than one thousand 3D printed components.[13]

4D printing, essentially 3D printing with "smart" and "memory" materials, continues to be an area of substantial research focus and opportunity. It offers the potential to allow self-constructing structures,

---

[9] http://avr-aerospace.com/what-is-adaptive-manufacturing-exactly/
[10] https://en.wikipedia.org/wiki/Robotic_process_automation
[11] http://www.supplychainbrain.com/content/blogs/think-tank/blog/article/how-robotics-process-automation-is-transforming-supply-chains/
[12] http://www.zdnet.com/article/5-6-million-3d-printers-will-be-shipped-by-2019-gartner/
[13] https://3dprint.com/63169/airbus-a350-xwb-3d-print/

objects that adapt to their surroundings while added manufacturing efficiency; and, reduced manufacturing cost and pollution.

Bioprinting, including both 3D and 4D technologies, has tremendous potential to revolutionize healthcare. The Wake Forest Institute for Regenerative Medicine has already produced human-scale tissue constructs with structural integrity with a specialized 3D bioprinter able to print ears, muscles and jawbones.[14]

Some 4D bioprinting technologies go outside the medical field into the bioengineering domain with "Engineered Living Materials" for construction development already underway with the near-term vision to be able to grow materials on demand from precursors shipped to the site where they are needed. "As these materials will be alive they should be able to respond to changes in their environment and heal themselves in response to damage." [15]

Bioengineering and bioprinting also offer the opportunity for adversaries to use the technology for more nefarious purposes including synthetic virology, with the opportunity to artificially develop weaponized viruses using 3D and 4D technology for biological warfare purposes. It may also offer the opportunity to shorten the response time against both natural and manmade pathogens through allowing rapid development of potential cures, and subsequently may also offer some deterrent value.[16]

Development of these innovative manufacturing technologies is enabled by integration with machine learning, advanced data analytics, "edge-heavy" and cloud enabled high performance computing (HPC) to analyze industrial processes to identify and implement efficiencies and cost-saving. It is now relatively economical to have a world class HPC platform, in the hundreds of Teraflops processing range, supporting industrial analysis and processing at the individual factory level. Manufacturing systems will be connected to complex Artificial Intelligence/HPC environments that also present a tempting target for non-state cyber adversaries who may seek to use their computational power and connectivity to enable operational activities such as password cracking and cryptographic analysis. This increasing capability and dependence means countries like North Korea, for example, that do not possess a significant high-tech manufacturing base could stage attacks against our industrial base and that of our industrialized allies without an equivalent adversary infrastructure to leverage a proportionate response against.

Any digital, interconnected technologies come with significant risk due to their attack surface and those faced by adaptive manufacturing are consistent with those faced by other CPS including Industrial Controls Systems (ICS) and Internet of Things (IoT) devices. Similarly, these risks extend beyond just the cyber networks into the wireless systems in and used for communications by industrial robots and machinery.

---

[14] http://cellculturedish.com/2016/01/another-perspective-on-4d-bioprinting/
[15] https://disruptionhub.com/5330-2/
[16] http://bio-defencewarfareanalyst.blogspot.com/2014/02/how-3d-bioprinting-would-change-wargame.html

Adaptive manufacturing systems offer tempting targets to nation state, terrorist, criminal, activist and opportunist adversaries for objectives including, but not limited to:

- Theft of trade secrets and intellectual property for economic advantage,
- Compromise to later conduct disruptive attacks for economic, issue motivated, political or military purposes,
- Manipulation or disruption of manufacturing processes and the supply chain for economic, issue motivated, political or military purposes,
- Manipulation of manufacturing processes to introduce vulnerabilities and flaws for economic, issue motivated, political or military purposes, and
- Misuse through use of the technology to manufacture contraband items, including weapons, outside of established and monitored channels.

Adversaries of the United States, including but not limited to Russia, China, Iran and North Korea, have all demonstrated the willingness and capability to conduct intrusions in network supporting CPS, staging capabilities to map and identify vulnerabilities in ICS networks in the electricity and other sectors.

An example of this kind of targeting was the compromise of websites of three security and industrial technology manufacturers to allow embedding of the Havex Trojan into firmware device updates to compromise targeted critical infrastructure and industrial control environments.[17] Victim environments reportedly compromised in this campaign included two German industrial technology producers; one French industrial manufacturer; two major French educational institutions that are known for technology-related research; and one Russian construction company that appears to specialize in structural engineering. [18]

A further example of the threat to automated manufacturing systems was reported by the German Federal Office for Information Security (or BSI) in December 2014.[19] The unidentified attackers gained access to the steel mill through the unnamed company's corporate network, then successively moved laterally through multiple systems into the connected industrial production network. "Failures accumulated in individual control components or entire systems" resulting in the plant being "unable to shut down a blast furnace in a regulated manner" with the result of "massive damage to the system." BSI stated the attackers appeared to possess advanced knowledge of industrial control systems. Bloomberg reporting alleges the activity had been linked to Russian espionage activity.[20]

The vulnerability of the wireless communications systems used by CPS was highlighted in an attack on a sewage treatment facility in Australia in 2000 when an attacker used a radio system, laptop and ICS

---

[17] https://ics.sans.org/blog/2016/04/25/fourth-sample-of-ics-tailored-malware-uncovered-and-the-potential-impact
[18] https://www.f-secure.com/weblog/archives/00002718.html
[19] https://www.wired.com/wp-content/uploads/2015/01/Lagebericht2014.pdf
[20] https://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato

software to wirelessly hack into the facility's control systems and discharge millions of gallons of sewerage into parks and water course significantly damaging the surrounding environment.[21]

At least one case of manufacturing supply chain manipulation by cyber means for economic gain has been reported by trusted sources for the purposes of devaluing a company for the purpose of international acquisition by a foreign company. This motivation has not been previously reported however presents a clear threat to companies that do not adequately protect their supply, production and distribution channels.[22]

Another risk associated with Adaptive Manufacturing processes is the potential to compromise and access the massive amounts of data generated during the design and production processes. These "digital threads" of interrelated information that run through the object's lifespan may contain a level of detail that could potentially aid attackers in identifying significant vulnerabilities in products.[23] Given access to appropriate resources, adversaries may use analytic and machine learning techniques to support this vulnerability analysis. Defensively, manufacturers should employ similar techniques to "red team" vulnerability analysis to enable early identification and mitigation of systemic vulnerabilities before an adversary is able.

One area of public and DHS concern in relation to 3D printing has been the threat of printing weapons, particularly hand guns, semiautomatic/automatic rifles and machine guns. There have been handgun and automatic weapon receiver models[24] shared and successfully printed but the limiting factor in these examples has been the strength and thermal characteristics of the publicly available thermoplastic printing materials, which have generally failed significantly when the weapon is fired due to the inability to cope with the pressure and temperature from standard ammunition. Most functioning printed weapons have had to have metals components constructed to handle the firing stresses, although at least one individual has developed special ammunition which makes printed handguns more viable.[25] Until stronger 3D printing materials become available, the threat of 3D printed guns must be considered low as it is much easier and cheaper to acquire standard firearms legally, or illegally, through existing channels. As we look towards 2021 however, with much stronger plastic printing materials becoming available, the evolving threat of 3D printed weapons must be considered medium to high.

All the previously described technologies offer the opportunity for significant societal and economic change and disruption. We have already seen the ability of technological advancement to displace those

---

[21] https://pdfs.semanticscholar.org/78df/bff3c64097ef061035839b7254f7f4dceacd.pdf
[22] http://www.ey.com/publication/vwluassets/ey-global-information-security-survey-2015/$file/ey-global-information-security-survey-2015.pdf
[23] John Hagel III et al., The future of manufacturing, Deloitte University Press, March 31, 2015, http://dupress.com/articles/future-of-manufacturing-industry/, December 13, 2015; Mark J. Cotteleer, Stuart Trouton, and Ed Dobner, 3D opportunity and the digital thread, Deloitte University Press, March 3, 2016, http://dupress.com/articles/3d-printing-digital-thread-in-manufacturing/
[24] https://en.wikipedia.org/wiki/List_of_3D_printed_weapons_and_parts
[25] http://mashable.com/2014/11/06/bullets-3d-printed-gun/

in the workforce who are not educated and equipped to adapt to rapid technological change. This will cause distress, and potentially social unrest, in those communities displaced by the implementation of advanced adaptive manufacturing technologies.

Recommendations

There are common threads of autonomy, artificial intelligence, interconnectedness through the Internet of Things and cybersecurity which permeate the domain of adaptive manufacturing. These interrelationships need to be understood and embraced to allow the coordination and integration necessary to deal with the vulnerabilities and opportunities presented by these domains.

The rapidity with which adaptive manufacturing technologies will evolve could itself pose a risk for the Homeland. Without appropriate technology monitoring and intelligence collection, it appears highly likely that disruptive breakthroughs in all areas of adaptive manufacturing may occur in the next five years posing potential economic and homeland security risks. DHS must work with appropriate private and government partners to ensure visibility of technological breakthroughs that could threaten the Homeland.

The Information and Communications Technology (ICT) security challenges facing adaptive manufacturing technologies are similarly not unique and are faced by all cyber-physical systems. There is a clear need for the Department of Homeland Security to work with the National Institute for Standard's and Technology (NIST) and relevant Departments and agencies to develop mandatory cybersecurity standards for CPS like those being developed by the Federal Aviation Administration for the aviation industry, based on recent incidents highlighting the vulnerability of aircraft interconnected systems.[26] NIST Special Publication 800-82, Revision 2, *"Guide to Industrial Control Systems (ICS) Security"* May 2015 [27] together with the recently updated NIST Cybersecurity Framework[28] offer excellent starting points for developing these standards. These guidelines do not clearly address the complexity or vulnerability of supply chain interdependencies for adaptive and other automated manufacturing process.

The recent media reporting that the United States has allegedly been developing disruptive and destructive cyberwarfare capabilities for attacking ICS and CPS.[29] While seeking to comment on those reports, it is clear a variety of adversaries will have taken those allegations seriously and will be building and expanding cyber-attack capabilities against a variety of CPS including those used in critical infrastructure. Without mandatory standards for CPS the likelihood of a catastrophic cyber-enabled physical event within the next five years grows increasingly likely.

---

[26] http://www.nextgov.com/cybersecurity/2016/03/faa-has-started-shaping-cybersecurity-regulations/126449/
[27] http://dx.doi.org/10.6028/NIST.SP.800-82r2
[28] https://www.nist.gov/cyberframework/draft-version-11
[29] http://www.businessinsider.com/nitro-zeus-iran-infrastructure-2016-7

Some recommendations are clearly beyond scope of DHS. DHS must work with the National Security community to define "Red lines" which are clearly communicated to foreign countries and potential non-state actors that indicate what would trigger a coordinated and definitive response by the US to hostile attacks on our manufacturing sector and other critical infrastructure sectors.[30]

[30] http://www.c4isrnet.com/articles/cyber-red-lines-ambiguous-by-necessity