DEFENSE DOSSIER

February 2015

ISSUE 13

NANOTECHNOLOGY AND U.S. MILITARY POWER
KELLEY SAYLER

CYBER WEAPONS AND MILITARY CAPABILITIES: AN INTRODUCTION
PAUL ROSENZWEIG

ROBOTS, WAR, AND SOCIETY
CAMILLE FRANCOIS

TRANSFORMING DEFENSE: THE POTENTIAL ROLE OF 3D PRINTING
JENNIFER MCARDLE

TIME TO DEPLOY CONVENTIONAL PROMPT GLOBAL STRIKE
THOMAS SCHEBER

American Foreign Policy Council

DEFENSE DOSSIER

February 2015 ISSUE 13

1. From the Editors **2**
Ilan Berman and Rich Harrison

2. Nanotechnology and U.S. Military power **3**
How micro-tech can be harnessed by the American armed forces.
Kelley Sayler

3. Cyber Weapons and Military Capabilities: An Introduction **7**
It's the next great battlefield. Here's what you need to know.
Paul Rosenzweig

4. Robots, War, and Society **11**
How robotics will alter the modern battlefield, and American culture.
Camille Francois

5. Tranforming Defense: The Potential Role of 3D Printing **16**
Future printing technologies have the power to fundamentally alter defense.
Jennifer McArdle

6. Time to Deploy Conventional Prompt Global Strike **21**
An alternative to nuclear weapons deserves its day in the sun.
Thomas Scheber

American Foreign Policy Council

FROM THE EDITORS

Welcome to the February 2015 edition of the *Defense Dossier*, the quarterly e-journal of the American Foreign Policy Council (AFPC). In this issue, we focus on the intersection of high technology and national security, and on potential game-changing technologies that will have an impact on military affairs in the years ahead.

These include cyberspace, a domain that still has murky rules of engagement, but where interconnectedness has created new opportunities and vulnerabilities of the U.S. It also encompasses robotic warfare, which is changing the concept of combat autonomy, and re-defining where the "battlefield" actually is. Similarly, 3D printing and nanotechnology both have promising futures in military applications. Meanwhile, the U.S. is now grappling with non-nuclear ways to quickly react to crises around the world: scenarios that elevate the importance of the concept known as "prompt global strike."

As always, we hope you find the contents of this issue to be both important and illuminating.

Sincerely,

Ilan Berman
Chief Editor

Richard Harrison
Managing Editor

NANOTECHNOLOGY AND U.S. MILITARY POWER

KELLEY SAYLER

A number of innovative technologies, ranging from tiny unmanned systems to real-time human performance enhancement, are likely to have a significant impact on the future of warfare and thus, on the future of American national security. In many of these cases, groundbreaking work in the field of nanotechnology promises to enable the development of revolutionary military capabilities that could sustain the U.S. military advantage well into the future.

But while the United States has long enjoyed a lead in nanotechnology research, steady declines in government funding as well as increased international investments now threaten to displace U.S. primacy in the field. Given both the past yields of nanotechnology research and its role in enabling the disruptive military technologies of the future, it will be critical for the United States to preserve federal funding for nanotechnology research and to further incentivize research conducted by educational institutions and private industry.

NANOTECHNOLOGY IN THE UNITED STATES

Recognizing the potential value of nanotechnology applications in both the civil and military spheres, the United States established the National Nanotechnology Initiative (NNI) in 2001 to promote and coordinate nanotechnology research and development across a number of government agencies. Since then, it has invested nearly $21 billion in federal nanotechnology research, including $1.5 billion in FY 2014. Of FY14 investments, roughly $156 million was devoted to research conducted by Defense Department (DoD) entities or partners, including DARPA, the Chemical and Biological Defense Program, the Defense Threat Reduction Agency (DTRA), and the Institute for Soldier Nanotechnologies—a joint enterprise between Massachusetts Institute of Technology and the U.S. Army.[1]

As articulated in the NNI Strategic Plan, much of DoD's current funding is devoted to improving sensors, advancing materials science, and increasing energy efficiency—all of which hold significant potential for strengthening U.S. warfighting capabilities and national security. To this end, DoD is pursuing research on nanotechnologies like biomarkers and biosensors that monitor soldier health, fatigue, and cognition. Already, the Army Research Laboratory has demonstrated applications for biosensors in the detection of mild traumatic brain injury—a capability that could dramatically improve injury diagnostics for forward deployed troops in theater—while the Institute for Soldier Nanotechnologies is continuing research into battlefield treatments for open wounds and hemorrhagic shock, a major cause of combat fatalities.[2]

DoD is also researching sensors that detect and protect against environmental threats, including chemical and biological agents as well as other hazardous pathogens. Ultimately, advancements in nanotechnology are expected to not only identify such threats but also enable point-of-care delivery of medicines, vaccines, and antidotes via wearable patches. Nanobiology research may also eventually produce neural implants that can treat post-traumatic stress disorder and restore or improve memory in warfighters.[3] Such technology, for which DARPA and other agencies maintain major research initiatives, could pave the way for more extensive forms of human performance enhancement.

Materials science is another NNI research priority that holds significant military utility. As part of this initiative, DoD is currently studying applications for graphene,

Kelley Sayler is a research associate with the Defense Strategies and Assessments Program at the Center for a New American Security.

a highly conductive material composed of carbon atoms that, despite being six times lighter than steel, is roughly 200 times stronger. While graphene is difficult to produce and prohibitively expensive at present, the material's unique characteristics are being explored for use in advanced night vision systems and flexible, water-proof electronics (e.g., foldable computers).[4]

Nanobiology research may also eventually produce neural implants that ... could pave the way for more extensive forms of human performance enhancement.

Materials with similar albeit slightly inferior properties have already met promising benchmarks. For example, in early testing, armor composed of carbon nanotubes (CNT) achieved technological readiness level 6 (successful demonstration in a relevant environment). This CNT-based armor weighed 10-19% less than traditional hard armor and 30% less than traditional soft armor, and is thought to be capable of achieving weight reductions of up to 80%.[5] If further developed, such materials could dramatically improve force protection and increase survivability while also reducing both weight burdens and cost. Significant reductions in weight could additionally improve vehicle speed and agility across the services.

Materials science has also yielded breakthroughs in active camouflage that is capable of automatically altering its appearance in response to changes in its environment. While this technology is not yet deployable in the field, researchers sponsored by the Office of Naval Research recently created a material that reacts and adapts to light sources—a first step in developing more advanced camouflage for warfighters. At a more speculative level, nanotechnology research could enable cloaking devices that refract light, effectively rendering the subject invisible. Such devices could be used to conceal individual warfighters as well as major weapons platforms.

Nanotechnology research could enable cloaking devices that refract light, effectively rendering the subject invisible.

Finally, the NNI is exploring nanotechnology as a means of generating and storing energy. To this end, small semiconductor particles called quantum dots have been used in an experimental capacity to improve energy efficiency by more than 40%, while carbon nanostructures and silicon have been used to increase battery storage and cost efficiency. These technologies in turn strengthen energy independence for permanent military installations and forward operating forces alike—in the case of the latter, reducing reliance on potentially vulnerable supply chains and enabling longer deployment cycles.

Past U.S. investments in nanotechnology have proved fruitful as well. In particular, DARPA's nano air vehicle program, which developed a 19-gram flying surveillance robot, demonstrated technologies that could provide the U.S. military with a critical advantage in reconnaissance and situational awareness, particularly in urban environments or other restricted-access areas.

Such advancements in miniaturization have also enabled the creation of nano quadrotors that can fly autonomously in formation and may one day be deployed on the battlefield as part of a robotic swarm. [6] This technology holds the potential to dramatically alter the offense-defense balance in military engagements—and with it, the character of warfare—by allowing for the coordination of large numbers of autonomous air vehicles that can, in turn, be utilized to degrade or destroy adversary defenses. Today, a public-private consortium led by the University of Pennsylvania's GRASP Laboratory is spearheading this research.

Indeed, in addition to the foundational research funded by the U.S. government, U.S. educational institutions and private industry are continuing research into nanotechnologies with significant military application. Though federal support for these activities continues to decline, U.S. corporate spending is on the rise, reaching $4.1 billion in 2012—an 11% increase over 2011 levels.[7]

A COMPETITIVE GLOBAL ENVIRONMENT

The United States remains the leading investor in nanotechnology research, despite recent declines in funding. But as foreign governments come to see the significant potential of both military and civilian applications of nanotechnology, the United States' lead will continue to narrow. Since 2012, overall U.S. funding for nanotechnology research has declined by 17%. For defense-specific research, which has declined by a remarkable 59% since 2012, the outlook is even more concerning.[8]

As foreign governments come to see the significant potential of both military and civilian applications of nanotechnology, the United States' lead will continue to narrow.

This is particularly the case because global spending on nanotechnology—including investments from governments, industry, and venture capitalists—rose by an estimated 40% per year between 2010 and 2013, and shows no signs of slowing.[9] Today, over sixty countries have federally funded nanotechnology programs, with Japan ($1.3 billion), Russia ($974 million), and Germany ($617 million) trailing the United States, according to open source data.[10]

Though it is difficult to obtain comprehensive, country-specific information about foreign funding for nanotechnology research, it is possible to assess the comparative interest in and maturity of national research programs by examining two proxy metrics: the number of nanotechnology papers published and the number of nanotechnology patents granted.

In the case of the former, the United States has lagged behind the European Union by a considerable margin for a number of years. Furthermore, given the exponential increase in the publication of Chinese papers since the early 2000s, the United States now additionally trails China, which overtook the European Union in net output in 2013.[11] Despite this, the U.S. maintains its advantage in number of patents granted—a telling measure of innovation—securing more than its closest competitors Japan, South Korea, Germany, and France.

While little is known about the research priorities of U.S. competitors, it must be assumed that at least some portion of their nanotechnology research is devoted to technologies with potential military utility, including nano air vehicles, hardened weapons platforms, and miniaturized weapons of mass destruction. Thus, without sustained commitment to nanotechnology research, the United States could become increasingly vulnerable to disruptive foreign military technologies.

MAINTAINING THE EDGE

Nanotechnology serves as a critical enabler and force multiplier for the U.S. military, offering substantial improvements in force protection, human performance enhancement, energy security, and offensive combat power, among a number of other areas. The U.S. lead in nanotechnology research is dwindling, however, as foreign governments expand their investments in the field. If the United States wishes to sustain its advantage in nano-enabled military technologies in the years to come, it must redouble its commitment to the NNI, restore funding for defense-specific programs, and further incentivize educational institutions and private industry to pursue independent nanotechnology research.

A failure to do so could cede crucial innovations to U.S. competitors and jeopardize the future of American military primacy.

ENDNOTES

[1] National Science and Technology Council Subcommittee on Nanoscale Science, Engineering, and Technology, The National Nanotechnology Initiative: Supplement to the President's 2015 Budget, March 2014.
[2] See "Project 2.3.2: Multi-component Nanolayer Assemblies for Soldier Wound Healing," Institute for Soldier Nanotechnologies, n.d., http://isnweb.mit.edu/project-2.3.2.html; See also "Project 2.3.1: Nano-structured Biomaterials for Treatment of Hemorrhagic Shock," Institute for Soldier Nanotechnologies, n.d., http://isnweb.mit.edu/project-2-3-1.html.
[3] See "Restoring Active Memory (RAM)," DARPA, n.d., http://www.darpa.mil/Our_Work/BTO/Programs/Restoring_Active_Memory_RAM.aspx; See also The White House, "BRAIN Initiative," September 30, 214, http://www.whitehouse.gov/share/brain-initiative.
[4] See "Project 1.2.1: Graphene Devices for Next-Generation Night Vision Systems," Institute for Soldier Nanotechnologies, http://isnweb.mit.edu/project-1-2-1.html.
[5] National Science and Technology Council, The National Nanotechnology Initiative: Supplement to the President's 2015 Budget; National Science and Technology Council Subcommittee on Nanoscale Science, Engineering, and Technology, The National Nanotechnology Initiative: Strategic Plan, February 2014, 17.
[6] See "A Swarm of Nano Quadrotors," Youtube.com, January 31, 2012, https://www.youtube.com/watch?v=YQIMGV5vtd4.
[7] Executive Office of the President, President's Council of Advisors on Science and Technology, Report to the President and the Congress on the Fifth Assessment of the National Nanotechnology Initiative, October 2014.
[8] National Science and Technology Council, The National Nanotechnology Initiative: Supplement to the President's 2015 Budget; National Science and Technology Council Subcommittee on Nanoscale Science, Engineering, and Technology, The National Nanotechnology Initiative: Supplement to the President's 2014 Budget, May 2013.
[9] "Market report on emerging nanotechnology now available," National Science Foundation, February 25, 2014, http://www.nsf.gov/news/news_summ.jsp?cntn_id=130586.
[10] Executive Office of the President, Report to the President and the Congress.
[11] Ibid.

CYBER WEAPONS AND MILITARY CAPABILITIES: AN INTODUCTION

PAUL ROSENZWEIG

What is the current state of U.S. and foreign cyber weapon capabilities? How do those respective capabilities impact U.S. national security? These are questions of grave consequence. Yet they are surprisingly difficult to answer. A survey of "learned scholarship" from across the globe can provide one with every opinion, ranging from "cyber war is a myth"[1] to a "cyber Pearl Harbor" is imminent.[2] As with most such issues, the answer lies somewhere between.

CYBER RISK TODAY

If you ask government professionals, they will tell you that America's critical infrastructure is highly vulnerable to attack. When he testified before the House Permanent Select Committee on Intelligence in November of 2014, NSA Director Admiral Michael Rogers asserted that several foreign countries, including China, have infiltrated the computers of critical industries in the United States to steal information that could be used in the planning of a destructive attack. They have, he said, done reconnaissance and even stolen the schematics of particular systems.[3] These concerns echoed an earlier report from the Department of Homeland Security, which took note of a hacking campaign attacking our nation's critical infrastructure. It has been ongoing since 2011, the study outlined, but no attempt has been made to activate the malware to "damage, modify, or otherwise disrupt" the industrial control process of our vital industries. Troublingly, U.S. officials only recently became aware of the penetration, and they reportedly still don't know where or when it may be unleashed.[4]

The result is, in many ways, deeply problematic—we are in the midst of a low-grade cyber conflict with other nation states, and yet we don't even know how to characterize what that conflict entails or how it is happening. Nor do we know what our opponents' objectives are. The best we can do is try and understand their capabilities. With that in mind, consider the cyber capabilities of the United States and some of our peer nation-state competitors.[5]

Russia[6]

Russia is better at cyber conflict than China—indeed, some of its capabilities are superior to those of the United States. The ground for this lies in the unique structure of Russian cyber capabilities. They reside not exclusively in independent military units but also within a cadre of highly talented criminal hackers—what David Smith (an observer of Russian capabilities) call the "unique nexus of government, business, and crime."[7] These criminals create, sell, and use advanced cyber tools for profit and are often at the cutting edge of new, advanced skills and weapons that increase Russia's cyber capabilities.[8] The Russian government has a symbiotic relationship with the criminal networks, permitting their "for-profit" criminality in exchange for their support in national conflicts such as those with Georgia and Estonia,[9] and more recently with Ukraine.

For these reasons, many observers think that Russian capabilities are almost equivalent to those of the United States. That, for example, is the opinion offered by the Director of National Intelligence in his recent Worldwide Threat Assessment delivered to Congressional lawmakers, and by the cybersecurity firm, FireEye, which described Russian cyber attacks as "techni-

***Paul Rosenzweig** is the Principal at Red Branch Consulting, a homeland security consulting firm, and a Senior Advisor to The Chertoff Group. He also serves as a Professorial Lecturer in Law at George Washington University where he teaches cybersecurity law and policy. He formerly was Deputy Assistant Secretary for Policy at the Department of Homeland Security.*

cally advanced and highly effective at evading detection."[10] Indeed, if you doubt the premise, one need only read the recent report from FireEye on a Russian program dubbed APT28, which has been systematically intruding on American governmental networks. [11]

Russia is better at cyber conflict than China — indeed, some of its capabilities are superior to those of the United States.

China

As recently as five years ago, the U.S. was unwilling to definitely accuse the Chinese government of a systematic cyber espionage campaign against American interests. As the Department of Defense's 2010 report to Congress on Military and Security Developments Involving the People's Republic of China carefully put it:

> …numerous computer systems around the world, including those owned by the U.S. government, continued to be the target of intrusions that appear to have originated within the [People's Republic of China]. These intrusions focused on exfiltrating information, some of which could be of strategic or military utility. The accesses and skills required for these intrusions are similar to those necessary to conduct computer network attacks. It remains unclear if these intrusions were conducted by, or with the endorsement of, the [People's Liberation Army] or other elements of the [People's Republic of China] government. However, developing capabilities for cyberwarfare is consistent with authoritative [People's Liberation Army] military writings.[12]

The lack of clarity in attribution has since faded quite a bit. Forensic efforts have identified at least one Chinese military unit with cyber intrusions.[13] In 2013, the Verizon Risk Center identified China as the "top external actor from which [computer] breaches emanated, representing 30 percent of cases where country-of-origin could be determined."[14] Indeed, the Verizon report concluded that China was the source of 95 percent of state-sponsored cyber-espionage attacks.

While it is certainly plausible that some of the hacks emanating from China are done without the government's knowledge, the frequency and persistence of the attacks, along with their political focus, clearly implicate Chinese involvement. As one analyst put it: "The Chinese government has employed this same tactic in numerous intrusions. Because their internal police and military have such a respected or feared voice among the hacking community, they can make use of the hackers' research with their knowledge and still keep the hackers tight-lipped about it. The hackers know that if they step out of line they will find themselves quickly in a very unpleasant prison in western China, turning large rocks into smaller rocks." [15]Indeed, the degree of intrusion has gotten so bad the corporate travelers heading to China now, routinely, take blank computers and never let their cell phones out of their possession. The Chinese reputation for routine hacking has become, in a word, legendary.[16]

Iran

Of all American nation-state competitors, only one has demonstrated a serious willingness to use cyber tools in disruptive kinetic ways against American targets: Iran. Cyber capabilities have been developed by the Iranian regime as a means of asymmetrically countering the technologically superior conventional weapons systems of the U.S., Israel, and others in the region. It began, in 2009, with the creation of Iranian Cyber Army.[17] In 2012, the Iranian annual budget for cyber capabilities was reported to be almost $1 billion.[18]

Of all American nation-state competitors, only one has demonstrated a serious willingness to use cyber tools in disruptive kinetic ways against American targets: Iran.

Iranian affiliated hackers have used cyber tools in a geo-strategic way to effect American and other interests. The most notable attack was a sophisticated and debilitating "distributed denial of service" DDoS attack on numerous U.S. banks in late 2012. Also in 2012, Iran was responsible for the "Shamoon" virus attack on Saudi Aramco, the world's largest oil producer, which destroyed around 30,000 computers, as well as an attack on the computer networks of Qatari natural gas company RasGas.[19]

United States

In response to all this, the Department of Defense has created its own cyberspace war-fighting unit, U.S. Cyber Command. The goal of this reorganization was to centralize a relatively decentralized military cyber effort and provide a unified command for both offensive and defensive operations. On the defensive side, Cyber Command is responsible for actions designed to "protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks."[20] Notably, though formally restricted to DoD systems, the Department has begun partnering with private sector manufacturers in the "Defense Industrial Base" to assure the security of its supply chain.

Offensive cyber operations can involve both information gathering (sometimes also called "computer network exploitation") and computer network attack. When an intrusion is for exploitation and information gathering purposes, the boundary between military operations and the espionage of the intelligence community gets blurred. Recognizing how espionage activities can blend into military operations that prepare the battlefield and involve reconnaissance, the commander of Cyber Command is also dual-hatted as the Director of the National Security Agency, our electronic intelligence gathering agency. Computer network attack involves military operations through computer networks that are designed to "disrupt, deny, degrade, or destroy information residing in computers and computer networks or the computers and networks themselves."[21] It may even involve exploitations that are intended to have destructive kinetic effects on hard military or civilian infrastructure targets. All of these fall within the purview of the new command.

At the beginning of 2014, Cyber Command had around 1,000 personnel to complete its mission. The first commander of Cyber Command, General Keith Alexander, predicted an increase in CYBERCOM personnel to approximately 1,800 by the end of 2014, while former Defense Secretary Chuck Hagel and others have stated that it will reach as many as 6,000 personnel in 2016.[22] Meanwhile, Cyber Command has seen its unclassified budget grow from $114 million in FY 2010 to $562 million in FY 2014.[23]

BEST DEFENCE

As the forgoing suggests, we are in the midst of a cyber arms race of sorts, but we don't even really know exactly what type of war we are fighting. Nor are we sure of the opponent's capabilities or their intentions. The challenge of cyber conflict is as much in trying define it as in trying to wage it—and we are only at the beginning of that process.

END NOTES

[1] Thomas Rid, "Think Again: Cyberwar," Foreign Policy, March/April 2012, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar.

[2] U.S. Department of Defense, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security," October 11, 2012, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

[3] Ellen Nakashima, "Foreign Powers Steal Data on Critical U.S. infrastructure, NSA Chief Says," Washington Post, November 20, 2014, http://www.washingtonpost.com/world/national-security/nsa-chief-foreign-powers-steal-data-on-critical-us-infrastructure/2014/11/20/ddd4392e-70cb-11e4-893f-86bd390a3340_story.html.

[4] Jack Cloherty and Pierre Thomas, "'Trojan Horse' Bug Lurking in Vital US Computers Since 2011," ABC News, November 6, 2014, http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476.

[5] We leave aside completely in this discussion the capabilities of non-state actors (either terrorist groups or hacktivists). Today, it is fair to say that their capabilities are less than those of sovereign nations, but one suspects that this state of affairs will not last for too much longer.

[6] For the country reviews of Russia, China, and Iran I have relied, in part, on research by my Heritage colleague, David Inserra, to whom I am indebted. His work will be part of a larger Heritage project on comparative global military capabilities. See "The Index of U.S. Military Strength - 2015" (unpublished draft, 2014).

[7] David J. Smith, "Russian Cyber Capabilities, Policy, and Practice," inFocus Quarterly, Winter 2014, http://www.jewishpolicycenter.org/4924/russian-cyber-capabilities.

[8] Ibid.

[9] Brian Krebs, "Mapping the Russian Business Network," Washington Post, October 13, 2007, http://voices.washingtonpost.com/securityfix/2007/10/mapping_the_russian_business_n.html; Peter Warren, "Hunt for Russia's Web Criminals," Guardian (London), November 14, 2007, http://www.theguardian.com/technology/2007/nov/15/news.crime.

[10] James R. Clapper, Unclassified Statement for the Record on the Worldwide threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence, January 31, 2014, http://www.intelligence.senate.gov/120131/clapper.pdf; Kenneth Geers, Darien Kindlund, Ned Goran, and Rob Rachwald, "World War C: Nation-State Motives Behind Today's Advanced Cyber Attacks," FireEye, September 30, 2013, http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf.

[11] See FireEye, "APT28: A Window into Russia's Cyber Espionage Operations?" October 2014, http://www.fireeye.com/resources/pdfs/apt28.pdf.

[12] Department of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2010, 16.

[13] Dan McWhorter, "Mandiant Exposes APT-1—One of China's Cyber Espionage Units and 3000 Indicators," Mandiant, February 18, 2013.

[14] Stephanie Henry, "Verizon Report Describes Trends in International Data Breaches, China-Based Espionage," U.S.-China Business Council Washington Update, n.d., http://www.uschina.org/washington-update/verizon-report-describes-trends-international-data-breaches-china-based-espionage; Lucian Constantin, "Verizon: One in Five Data Breaches are the Result of Cyberespionage," PC World, April 23, 2013, http://www.pcworld.com/article/2036177/one-in-five-data-breaches-are-the-result-of-cyberespionage-verizon-says.html.

[15] Michael Joseph Gross, "Enter the Cyber-dragon," Vanity Fair, September 2011, http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109.

[16] Nicole Perlroth, "Electronic Security a Worry in an Age of Digital Espionage," New York Times, February 10, 2012, https://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html.

[17] Nart Villeneuve, Ned Moran, Thoufique Haq, and Mike Scott, "Operation Saffron Rose," FireEye, 2014, http://www.fireeye.com/resources/pdfs/fireeye-operation-saffron-rose.pdf.

[18] Siobhan Gorman and Julian E. Barnes, "Iran Blamed for Cyberattacks" Wall Street Journal, October 12, 2012, http://online.wsj.com/news/articles/SB10000872396390444657804578052931555576700?mg=reno64-wsj.

[19] Christiopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," Survival 55, no. 2, April/May 2013, 81-96, http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272; "Our Company," Saudi Aramco, n.d., http://www.saudiaramco.com/content/www/en/home.html#our-company%257C%252Fen%252Fhome%252Four-company%252Fat-a-glance.baseajax.html.

[20] U.S. Government Accountability Office, "Defense Department Cyber Efforts," May 2011, 2–3, http://www.gao.gov/new.items/d1175.pdf.

[21] Ibid.

[22] Courtney Kube, "U.S. Cyber Defense Force to Hit 6,000 by 2016, Hagel Says," NBC, March 28, 2014, http://www.nbcnews.com/news/us-news/u-s-cyber-defense-force-hit-6-000-2016-hagel-n66571; Ellen Nakashima, "Pentagon Cyber Unit Wants to 'Get Inside the Bad Guy's Head," Washington Post, June 19, 2014, http://www.washingtonpost.com/news/checkpoint/wp/2014/06/19/pentagon-cyber-unit-wants-to-get-inside-the-bad-guys-head/; Ellen Nakashima, "Alexander: Promote Cyber Command to Full Unified Command Status," Washington Post, March 12, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/12/alexander-promote-cyber-command-to-full-unified-command-status/.

[23] Brian Fung, "Cyber Command's Exploding Budget, in 1 chart", Washington Post, January 15, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/15/cyber-commands-exploding-budget-in-1-chart/.

ROBOTS, WAR, AND SOCIETY

CAMILLE FRANCOIS

Since 2007, the discipline of military robotics has gained sustained and significant attention in the public debate. There is today a growing body of scholarly work devoted to the ethical implications of autonomy, remote warfare, and its compliance with the requirements of international humanitarian law.

Roboticists such as Ronald Arkin have argued that military robotics could yield new forms of conflict, more moral and more observant of international law. "[R]obots not only can be better than soldiers in conducting warfare in certain circumstances, but they can also be more humane in the battlefield than humans," he wrote in a piece describing current research underway to explore the implementation of "ethical governors" in robotic technologies.[1] Other scholars have responded that autonomous lethal weapons will never have the agency and morality needed to comply with the complexities of constraints on the use of force, notably as far as the principles of distinction, proportionality and the need for accountability are concerned.[2]

To date, there are no "fully autonomous" weapons (i.e., weapons that can select and engage targets without human intervention) currently deployed on any battlefield. But advances in engineering and software are bringing these weapons closer to reality—and of course, the use of "semi-autonomous" and remotely operated weapons is steadily increasing. Works such as P.W. Singer's *Wired for War*[3] have reached a wide audience and helped popularize these issues, which are also entwined in the public debate with unmanned aerial vehicles (UAV, or drones) and the legality of targeted killings.

A CHANGING DISCOURSE

"Robotic warfare" is quickly becoming a politicized term and these debates have spawned new coalitions and civil society organizations. Coalitions of scholars and human rights activists, such as the International Committee for Robot Arms Control (ICRAC), have formed to argue in favor of an international ban on autonomous lethal weapons.[4] The Campaign to Stop Killer Robots is a successful example of the migration of this originally academic and theoretical debate in the political sphere.[5] In May 2014, for instance, the United Nations Convention on Certain Conventional Weapons held a Geneva meeting on "Lethal Autonomous Weapons Systems," bringing killer robots into an international humanitarian concern that historically has addressed issues like landmines and blinding lasers.[6]

It will be hard, however, to separate either the strategic or human rights considerations of robotic warfare from the popular perception of "killer robots." Years of mainstream media have popularized a dystopian future in which robotic soldiers mow down human targets with brutal efficiency, commanded by a rogue artificial intelligence (AI). Perhaps the most prominent of these is the *Terminator* movie franchise, the plot of which is predicated on a military defense network ("Skynet") becoming self-aware and turning on its creators. That is a far-fetched scenario, yet business and science leaders have lent credence to these fears in recent years. Take rocket- and electric car investor Elon Musk, who has tweeted, with the casual brevity that befits that medium, that "We need to be super careful with AI. Potentially more dangerous than nukes."[7] Fears of rogue or malevolent AIs were later seconded by the famed physicist Stephen Hawking,

Camille François *is a fellow at the Harvard Law School Berkman Center for Internet & Society. She is a researcher, consultant and lecturer on cybersecurity policy, cyberwar and robotics issues.*

who warned in a BBC interview that developments in AI "could spell the end of the human race."[8]

These statements illustrate a new turn in the wider debate over robotic warfare. The topic matured politically on the international scene, and fears of the impact of military robotics development are now spreading to the public in a more structured and articulate way than previously observed. When reality catches up with our science fiction dreams and nightmares, the evolution of military robotics technology—and the legal and ethical framework within which it takes place—gains renewed interest. This is the ideal time to engage stakeholders across society to difficult, ambiguous questions surrounding the very real developments in robotic warfare.

A QUICKENING PACE

As new technologies such as robotics come to challenge our legal, policy and ethical frameworks, a strong dialogue between the military and other institutions will be essential. Norms and rules created in one domain will inevitably come to affect the others, especially when it comes to new technologies, which themselves circulate between military and civilian use to create a "feedback loop." Many modern technologies have stemmed from military research; the most common examples include the Internet, GPS and microwaves. Civilian technology also serves military purposes, and in the robotics industry it is very much the case that civilian innovation feeds into the military realm.

Take iRobot, a company founded in 1990 by three M.I.T. computer scientists. It produces both the popular plate-shaped vacuum cleaning "Roomba" robot and the military PackBot multi-mission robot notably used in Iraq and Afghanistan for improvised explosive device identification and disposal. On iRobot's website, products are showcased in different tables entitled "for the home," "for business" and "for defense and security."[9]

Civilian robotics companies have often walked this line, but many were stunned in late 2013 when Google announced its acquisition of Boston Dynamics, its eighth robotics company in a string of related acquisitions. Boston Dynamics is an engineering and robotics military contractor, best known for the BigDog—a quadruped robot designed for the U.S. military with funding from the Defense Advanced Research Projects Agency and the U.S. Army. In the months preceding this move, Google had already started this trend by hiring several key figures out of DARPA, including former Director Regina Dugan and hacker/innovator Peiter "Mudge" Zatko. Then, in January 2014, Google announced a $650 million acquisition of DeepMind, a company specializing in strong Artificial General Intelligence (AGI). As part of the acquisition, DeepMind set a condition that Google form an AI ethics committee to determine how its technology may and may not be used.

If Google and the broader private sector now drives a significant part of the robotics search — including military components — we can expect robots to deploy faster in society, both in markets and on the battlefield.

Google certainly won't turn into "Skynet" and soon begin building Terminator robots. But these moves aren't without consequences either. One should, for instance, expect that when leading military robotics research is transferred from military research agencies such as DARPA to Silicon Valley tech giants such as Google, the timeline in which research translates into deployment in markets will shorten. Google has a history and reputation of moving forward quickly in testing and deploying its innovations (such as self driving cars), whereas military research agencies tend to be more careful and circumspect, or at least to target deployment on the battlefield rather than in all realms of society (circulation of technology to law enforcement forces being a noted and controversial exception here). DARPA's mission, since its establishment in 1958 after the "surprise" launch of Sputnik, revolves around preventing technological surprises to the U.S. But as robotics research moves into the private sector, the incentives are different. In short, if Google and the broader private sector now drives a significant part of the robotics research—including in its military components—we can expect robots to deploy faster in society, both in markets and on the battlefield.

DEFINITIONS AND PARADOXES

As the space between civilian and military robotics shrinks, some of the common issues will be discussed in their broader societal context, which will surely make for a more productive and comprehensive conversation on key legal and ethical topics. Some elements, though, are likely to hamper productive conversations both within each realm (civilian and military) and across them both. One of note is the lack of clear definition for "robots" or "robotics."

"Robotic warfare" evokes the entangled concerns of cyber warfare, automation and human rights (to name just a few). In fact, we may say that "robot" is actually a helpful abstraction—and that "robotic warfare" is a convenient amalgamation of several different technologies and trends compressed into a single concept.

This begins with a lack of consistent terms of reference. Roboticists themselves are still struggling to set a definition. George Bekey's work on defining the contours of a robot provides a good foundation in this regard. He writes: "In its most basic sense, we define 'robot' as a machine, situated in the world, that senses, thinks and act."[10] The rapid pace of robotics innovation and the evolution of robotics forms (from biomimicry to human enhancements) make the definitional exercise quite a challenging one. As such, definitions continue to rest on unsatisfactory, essential descriptions of "machines of our creation."

Beyond "what's a robot," there also questions on "which robots are we concerned with" and "how do we talk about robots and robotics"? As mentioned, public debate has mainly concerned itself with autonomous systems. Yet autonomy, too, is a complicated concept to define. Going back to Bekey's definition: "Fully remote or teleoperated machines would not count as autonomous, since they fully depend on external control; they cannot 'think' and, therefore, cannot act for themselves."[11] Should our moral and legal norms, then, focus on certain characteristics of a robot that would make it undesirable and dangerous in and of itself (akin to weapons prohibited by international law that are considered malum in se)? Or should they instead rest on specific uses of said robots?

In more mainstream terms: what makes a good robot, and a bad robot? Is any robot equipped with high autonomy and strong AI a bad robot? Are autonomous robots bad if used in offense and good if used for defensive purposes? Much of the drone debate, for example, focuses on the lethal autonomous uses of the robots.

Military robotics also has plenty of non-lethal (and therefore more popular) robots assigned to protecting and "caring" for troops, such as the Battlefield-Extraction-Assist Robot (BEAR), tasked with extracting wounded soldiers from the battlefield with no risk to human life, or the BigDog robot which can walk alongside service members and serve as a robotic pack mule when terrain is too difficult for conventional vehicles. Such robots are often assigned to "3D jobs" (i.e, Dull, Dirty & Dangerous jobs).

Besides defining which robots we are talking about, there are concerns about how we talk about robots. Specifically, roboticists have noted that the trend of anthropomorphizing robots (which is truly a trend in both language and design) is counter-productive and even dangerous for thinking through legal, moral and policy issues in military robotics. Noel Sharkey, Professor of Artificial Intelligence at Sheffield University, explains that "[t]he myth of AI makes it acceptable, and even customary, to describe robots with an anthropomorphic narrative."[12] Sharkey refers to Drew McDermott's influential essay *Artificial Intelligence Meets Natural Stupidity*[13] and to the use of "wishful mnemonics" in the field of artificial intelligence, such as researching using words like understand to describe aspects of their programs. This leads us to mistakenly evaluate what robots can and cannot truly do. Simply put, if you call your robot "John Trooper" rather than "BBK-85," you will surely be more inclined to think robots could eventually act in a moral, legal and responsible way.

Another factor that will take more importance as the military robotics debate goes mainstream is the strategic paradox of the unintended consequences of robotic warfare. Robotic warfare's appeal is to distance troops from their target, making America's service members safer. Yet concerns have arisen that robotic warfare's unintended result is to bring the battlefield closer to, or even into, the homeland. U.S. Army Lieutenant Colonel Douglas A. Pryer's article in the *Military Review* on "why increasingly 'perfect' weapons help perpetuate our wars and endanger our nations" develops some key psychological and strategic reasons about why the rise of robotics doesn't necessarily contribute to a safer homeland.[14] His piece insists on robotic warfare yielding strong moral reprobation within civilian populations abroad, dangerously fueling anti-American sentiment and raising domestic threat levels. Others, such as Arizona State University's Braden Allenby, have worried that robotic warfare could expand the range of legitimate military targets out of the battlefield and into the homeland—to include, for instance, drone operators in Nevada, outside their hours of operation and into their homes. "With Napoleonic-era combat, you knew where the battlefield was, right? With modern warfare, modern conflict, you really don't know, where the battlefield is," Allenby explained to reporter Manoush Zomorodi.[15]

Robotic warfare's appeal is to distance troops from their target making America's service member's safer. Yet concerns ahve arisen that robotic warfare's unintended result is to bring the battlefield closer to, or even into, the homeland.

Military robotics will certainly not be contained on the battlefield, both because robotic warfare is likely to extend the very idea of a 'battlefield' and because of technology transfers with society.

These questions will need to be placed within the larger context of the evolving nature of battlefield in the age of asymmetric warfare and terrorism, and how new technologies force us to re-think the role of the military in securing society.

Military robotics, as a technology, will also easily find its way into society, both via dual-use technologies and through the use of the military robots for domestic security missions (such as immigration control and border patrols, for instance). In short, military robotics will certainly not be contained on the battlefield, both because robotic warfare is likely to extend the very idea of a 'battlefield' and because of technology transfers with society.[16]

HARD QUESTIONS

In the meantime, at home, parallel questions of robot ethics, accountability and liability take on great urgency as automation progresses and as robots spread into all areas of society. The year 2014 ended with a quite odd event, when Swiss artists deployed a bot programmed to randomly spend units of the virtual currency Bitcoin which returned with ecstasy pills and a fake Hungarian passport. In response, Ryan Calo, an expert in robotics-and-the-law issues, penned an opinion piece for *Forbes* smartly titled: "A Robot Just Committed a Crime. Now What?"[17] That is a question that the military has had on its desk for a little while now. But it only just arrived in Swiss art galleries.

With the acceleration of both the development of military robotics and of the pace at which it will impact all fields in society, the urgency of finding ways to engage in a productive debate about its legal and ethical impacts is great. Mapping how these technologies will spread, understanding how they will change society, breaking silos separating civilian and military thinkers along with addressing the lack of clear vocabulary to articulate these issues should be priorities.

ENDNOTES

[1] Ronald C. Arkin, "Ethical Robots in Warfare," IEEE Technology and Society Magazine, 2009.

[2] Noel E. Sharkey, "The Evitability of Autonomous Robot Warfare," International Review of the Red Cross 94, no. 886, Summer 2012, https://www.icrc.org/eng/assets/files/review/2012/irrc-886-sharkey.pdf.

[3] Peter W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century (Penguin Books, 2009).

[4] International Committee for Robot Arms Control (icrac.net)

[5] "2014 : A Year of Progress" Campaign to Stop Killer Robots, n.d., http://www.stopkillerrobots.org/2014/12/yearofprogress/.

[6] CCW Expert Meeting, "Lethal Autonomous Weapon Systems: Provisional Agenda," n.d.,

[7] http://unog.ch/80256EDD006B8954/(httpAssets)/58F0B0F7009B4407C1257CC4003382F2/$file/ProvisionalAgenda_LAWSMX_22April.pdf.

[8] Elon Musk, tweet on August 2, 2014, https://twitter.com/elonmusk.

[9] As cited in Rory Cellan-Jones, "Stephen Hawking Warns Artificial Intelligence Could End Mankind," BBC, December 2, 2014, http://www.bbc.com/news/technology-30290540.

[10] iRobot Corporation, www.irobot.com.

[11] George A. Bekey, "Current Trends in Robotics: Technology and Ethics," in Patrick Lin, Keith Abney and George A. Bekey, Robot Ethics: The Ethical and Social Implications of Robotics (Boston, MA: MIT Press, 2011).

[12] Ibid.

[13] Noel Sharkey and Lucy Suchman, "Wishful Mnemonics and Autonomous Killing Machines," AISB Quarterly no. 136, May 2013, 14-20, http://eprints.lancs.ac.uk/65657/1/Sharkey_Suchman_AISBQ_136.pdf.

[14] Drew McDermott, "Artificial Intelligence Meets Natural Stupidity," in John Haugeland, ed. Mind Design: Philosophy, Psychology, Artificial Intelligence (Cambridge, MA: MIT Press, 1981).

[15] Lieutenant Colonel Douglas A. Pryer, "The Rise of the Machines," Military Review, March-April 2013, 14-24.

[16] "New Tech City," WNYC podcast, October 1, 2014, http://www.wnyc.org/story/killer-robots-ancient-rules-war-trouble/.

[17] On this, see Patrick Lin, "Military 2.0.: Ethical Blowback from Emerging Technologies," Robots, Ethics & War blog, December 15, 2010, https://cyberlaw.stanford.edu/blog/2010/12/robots-ethics-war.

[18] Ryan Calo, "A Robot Really Committed A Crime: Now What?" Forbes, December 23, 2014, http://www.forbes.com/sites/ryancalo/2014/12/23/a-robot-really-committed-a-crime-now-what/.

TRANSFORMING DEFENSE: THE POTENTIAL ROLE OF 3D PRINTING

JENNIFER MCARDLE

"It ought to be remembered that there is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things. Because the innovator has for enemies all those who have done well under the old conditions, and lukewarm defenders in those who may do well under the new." – Niccolò Machiavelli, The Prince

A "disruptive technology"[1] ; the "third industrial revolution"[2] ; an element of "strategic latency,"[3] and; a game-changer in "tomorrow's wars, [where] battles will be fought with a 3D printer."[4] There seems to be no dearth of forecasts when it comes to describing the transformational potential of 3D printing. Indeed, the advent of 3D printing promises to touch and transform every facet of American life, including the military. For this reason, the U.S. government has been exploring mechanisms to harness this rapidly accelerating technology in order to best meet the warfighter's needs of the future. However, absent an effort on the part of the Department of Defense (DoD) to engage in a profound recasting of its organizational structure, 3D printing will not be leveraged to its full potential.

WHAT IS 3D PRINTING

3D printing, also known as additive manufacturing,[5] is a four-part manufacturing process whereby a computer-aided design (CAD) file, which is sliced up into a .STL file, guides a 3D printer to deposit a liquid polymer in a designated thin layer. The 3D printer then guides the "printer head" over the previous layer, stacking vertical layers of horizontally printed material until a 3D physical object emerges. [6]

3D printing is not a new technology. It has, in fact, been in development since the early 1980s, when Charles Hull—the "father" of 3D printing—started fabricating plastic devices from photopolymers and later patented stereolithography.[7] However, contemporary advances in additive manufacturing techniques, along with its growing commercial diffusion, have secured 3D printing's recent place on the emergent technology "hype cycle."[8]

As the Atlantic Council has noted, a "revolution is occurring at the high end and the low end [of the 3D printing spectrum], and converging towards the middle."[9] On the high end of the spectrum ($500,000+), gains are occurring in cutting-edge energy sources, new materials, such as metals, and complex algorithms; while the low end (<$500) is centered on creating greater consumer accessibility through decreased cost and complexity. These advances are ushering in new applications for 3D printing that many predict will have a disruptive impact across all sectors, including the military.

3D PRINTING IN THE MILITARY

In the last several years, the U.S. military has attempted to leverage the transformational potential of 3D printing, integrating 3D printed components into its weapon systems and altering aspects of its logistics and supply chain.

In 2012, the Army deployed Rapid Equipping Fielding (REF) expeditionary laboratories for rapid prototyping to Afghanistan. The REFs forward deploy

Jennifer McArdle is a Research Associate and Fellow in the Center for Revolutionary Scientific Thought at the Potomac Institute for Policy Studies.

teams of soldiers and engineers, which interface with military units, canvass the battlefield for emerging requirements, and facilitate rapid solutions for those emergent needs in theater.[10] REF solutions include battery adapters for increased battery lifetimes and protective caps for the Mine Resistant Ambush Protected (MRAP) vehicles' tire inflation systems, among others. However, despite REF success, the military is not yet able to print military-grade munitions.

Absent an effort on the part of the Department of Defense to engage in a profound recasting of its organizational structure, 3D printing will not be leveraged to its full potential.

The Navy has also forward deployed 3D printers on the USS *Essex*, an amphibious assault ship, with the hope of manufacturing on-board medical supplies. However, in the past year, junior sailors have produced more than plastic syringes and scalpels. 3D fabricated components have ranged from deck covers, to caps, and screws.[11]

Military contractors have also embraced the lure of 3D printing. Aerospace companies have drawn on additive manufacturing to fabricate prototypes, and many aircraft, such as the Boeing F-18 fighter, have 3D printed incorporated components, such as aircraft ducts.[12] The military and associated research universities have also begun to fabricate parts for unmanned aerial vehicles (UAVs). The X-47B UAV includes a 3D printed titanium air mixer and, perhaps more notably, the University of Virginia successfully printed an entire working UAV for the DoD.[13]

Despite these initiatives the military's current use of 3D printed components for weapon systems and forward deployed logistics does not even begin to scratch the surface of additive manufacturing's future potential.

IMAGINING THE MILITARY FUTURE OF 3D PRINTING

The military has begun to imagine a future whereby 3D printing is harnessed to completely remove supply chains, logistics, and even soldiers or sailors from the battlefield.

A 2013 U.S. Navy *Proceedings* article imagines a naval future characterized by a profoundly different logistics and construction process. The authors, Lieutenant Scott Cheney-Peters and Lieutenant Matthew Hipple, forecast future naval ships capable of harvesting the ocean for 3D printer materials, which would subsequently be manufactured into repair parts by additive manufacturing flotilla factories. Moreover, as the Navy continues to design innovative unmanned systems, for both ships and robotic crews,[14] Cheney-Peters and Hipple hypothesize that the future Navy may also be printing robotic crewmembers to fight and project power.[15]

That may be only the beginning. As electronic components continue along the trajectory of Moore's law—shrinking in size and increasing in computing power—the potential may exist for 3D printers to one-day print in voxels[16] containing tiny circuits. Just as integrated pixels led to an era of high-resolution digital images, "a perfect union of voxels would create intelligent, three-dimensional active physical objects."[17] In effect, "the future lies in programmable matter, raw materials whose behavior we can program and 3D print in a chosen shape."[18] This could have unbelievable implications for the 3D printed sailors that Cheney-Peters and Hipple imagined. As MIT professor Neil Gershenfeld

The military's current use of 3D printed components for weapon systems and forward deployed logistics does not even begin to scratch the surface of additive manufacturing's future potential.

notes, programmable matter will contain a mind of its own—it will be self-aware.[19] Instead of forward deploying soldiers, the military would have an in-theater, self-generating, self-aware, military capability, along with a seemingly endless supply of reserves.

Instead of forward deploying soldiers, the military would have an in-theater, self-generating, self-aware, military capability, along with a seemingly endless supply of reserves.

The list of potential future military applications of 3D printing goes on. The Army has been experimenting with everything from additive manufactured textiles for future combat fatigues to biogenetic materials and food.[20] There is no lack of potential 3D printing applications for the military. The main question is whether these future concepts can fully materialize.

TAKING ADVANTAGE OF SYSTEMIC CHANGE

Technological innovation, however, is not a sufficient condition for military disruption. If 3D printing is to bring truly revolutionary potential to the military, organizational reform in the DoD will need to take place in tandem with additive manufacturing innovation. Only then can the DoD leverage 3D printing's full potential to gain an enduring advantage over any putative peer competitor.

History demonstrates that military disruption arises from a combination of technological and organizational innovation. Indeed, in 1346, "it was not the intrinsic superiority of the longbow that won the Battle of Crécy [of the Hundred Years' War], but rather the way in which it interacted with the equipment employed by the French on that day and at that place."[21] Over a thirty-year period from 1850 to 1880, the French Navy was the first to invent shell guns, a steam powered warship, a mechanically powered submarine, a steel hulled battleship, and an ironclad warship. These innovations should have given the French Navy a war-fighting edge over its rival, the British Navy, yet they did not. As Michael C. Horowitz notes, "While the French excelled at inventing new technologies, crippling organizational debates prevented the integration of those technologies into French naval strategy."[22] Both the French and the British were the first-movers of armored warfare, yet it was the German development and marriage of a combined arms concept with lightning thrusts that altered the WWII European balance of power and forever cemented *blitzkrieg* warfare's place in history. Moreover, it was not the advent of the aircraft carrier that transformed naval warfare during WWII, but the U.S. and Japanese use of naval air power based on carriers that accompanied their fleets into battle.[23]

If the DoD is to successfully harness major technological innovations, such as additive manufacturing, it will need to engage—in parallel, rather than in a sequential fashion—in a process of organizational reform. This will be a difficult task. After all, as Max Weber once argued, "the essence of bureaucracy [is] routine, repetitive, orderly action."[24] Large bureaucracies, like the DoD, are ponderous, slow-moving beasts. Accordingly, the DoD needs to start considering how it can best integrate 3D printing into the defense apparatus and service organizations in order to fully exploit its potential for the wars of tomorrow.

LEVERAGING POTENTIAL

As an initial step, the DoD should establish a coordinating body, or a "3D printing czar,"[25] within the Pentagon. This additive manufacturing "czar" would have two main tasks: to develop a clear strategy for 3D printing in the military and to interface and coordinate across all relevant additive manufacturing entities, to include industry, academia, the National Network for Manufacturing Innovation,[26] and the three services and their associated laboratories.

A natural home for a 3D printing "czar" would be in the Office of Emerging Capability and

Prototyping (EC&P) under the Office of the Secretary of Defense.[27] The mission of the EC&P is to identify, develop, and demonstrate multi-domain concepts and technology for the immediate and future needs of DoD and its service organizations. Housing a 3D printing "czar" or coordinating body within the EC&P would yield several benefits:

- The EC&P is overseen by the Assistant Secretary of Defense for Research and Engineering (ASD[R&E]). The ASD(R&E) maintains strong connections across the military, government, and commercial laboratories, which the additive manufacturing "czar" could thereby leverage. Moreover, the ASD(R&E) is knowledgeable of each service's war-fighting mission and culture, and therefore will be best able to ensure that efforts are not duplicated across the services.

- Furthermore, being overseen by the ASD(R&E) will help ensure a strong connection to the Joint Staff, and through them the combatant commands, which can help identify persistent and pervasive warfighter problems.[28] This would allow the ASD(R&E) and the additive manufacturing "czar" to think strategically about how best to utilize 3D printing to address those challenges and potential future threats.

Technology is inherently a key facet of war, but technological change, in and of itself, does not suffice to bring about successful military innovation. The military will only reap the full benefits of these forecasted technological futures by engaging in meaningful bureaucratic reform.

ENDNOTES

1 James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs, "Disruptive Technologies: Advances that will transform life, business, and the global economy," McKinsey Global Institute (May, 2013).

2 "Additive Manufacturing: Sold Print," The Economist, April 21, 2012.

3 Banning Garret, "3D Printing: More Opportunities Than Dangers," in Zachary Davis, Ronald Lehman, and Michael Nacht, Strategic Latency and World Power: How Technology is Changing our Concepts of Security (Lawrence Livermore Laboratory: Center for Global Security Research, 2014).

4 Robert Beckhusen, "In Tomorrow's Wars, Battles will be Fought with a 3D Printer," Wired, May 17, 2013.

5 Other terms for 3D printing exist, such as rapid prototyping or solid-freeform technology. However, for the purpose of this article the author has selected to use the two terms that appear most frequently in the media interchangeably (3D printing and additive manufacturing).

6 See Hod Lipson and Melba Kurman, Fabricated: The New World of 3D Printing (Indianapolis: John Wiley & Sons, 2013), 12, and Bethany C. Gross, Jayda L. Erkal, Sarah Y. Lockwood, Chengpeng Chen, and Dana M. Spence, "Evaluation of 3D Printing and Its Potential Impact on Biotechnology and the Chemical Sciences," Analytical Chemistry 86, January 2014, 3242. Multiple methods of additive manufacturing exist. The description above outlines a method known as stereolithography. There are also methods of selective laser melting, fused deposition modeling, inkjet head printing, and electron beam melting. For more information on these methods, see "The Renaissance in Additive Manufacturing is Now," in Bob Hummel, ed., Alternative Corrosion Futures (Arlington, Potomac Institute for Policy Studies, 2014) 167.

7 For a concise historical perspective, see Gross et al., "Evaluation of 3D Printing and Its Potential Impact on Biotechnology and the Chemical Sciences."

8 Pete Basiliere and Michael Shanler, "Hype Cycle for 3D Printing, 2014," Gartner, July 21, 2014.

9 Thomas Campbell, Christopher Williams, Olga Ivanova, and Banning Garrett, "Could 3D Printing Change the World? Technologies, Potential, and Implications of Additive Manufacturing," Strategic Foresight Initiative, October 2011, 5.

10 Adam Asclipiadis, "Rapid Equipping Force uses 3D printing on the frontline," army.mil, July 9, 2014, http://www.army.mil/article/129635/Rapid_Equipping_Force_uses_3_D_printing_on_the_frontline/

11 Meghann Myers, "Sailors design parts on gators 3-D printer," Navy Times, May 18, 2014.

12 "Additive Manufacturing: Solid Print," The Economist, April 21, 2012; Aaron Martin and Ben Fitzgerald, "Process over Platforms: A Paradigm Shift in Acquisition through Advanced Manufacturing," Center for a New American Security CNAS Disruptive Defense Papers December 2013.

13 Jordan Golson, "A Military-Grade Drone that can be Printed Anywhere," Wired, September 16, 2014.

14 Researchers at the U.S. Naval Research Laboratory, Virginia Tech, and the University of Pennsylvania are developing an Autonomous Shipboard Humanoid (ASH), designed to walk in any direction, balance at sea, and navigate the small passageways and ladders of naval vessels. Moreover, the ASH will be capable of firing propelled extinguishing agent technology grenades, and use hoses and fire extinguishers. See Al Kamen, "Wanted: Robot Pitcher," Washington Post, October 9, 2012.

15 Scott Cheney-Peters and Matthew Hipple, "Print Me a Cruiser," Proceedings 139, iss. 4, April 2013.

[16] Voxel, which is a combination of the terms "volume" and "pixel," represents a value, or a single data point, on a regular grid in three-dimensional space.
[17] Hod Lipson and Melba Kurman, Fabricated: The New World of 3D Printing (Indianapolis: John Wiley & Sons, 2013), 17.
[18] Ibid.
[19] For more information, see Neil Gershenfeld, When Things Start to Think (New York, NY: Henry Holt & Company, 1999).
[20] For more information, see "Focus: 3D Printing," Army Technology 2, no. 4, July/August 2014, and; Chris Anderson, Makers: The New Industrial Revolution (New York, Crown Publishing Group: 2012).
[21] Martin Van Creveld, Technology and War: From 2000 BC to the Present (New York: The Free Press, 1991), 319. From Terry Pierce, Warfighting and Disruptive Technologies: Disguising Innovation (New York: Frank Kass, 2004), xii.
[22] Michael C. Horowitz, The Diffusion of Military Power: Causes and Consequences for International Politics (Princeton: Princeton University Press, 2010), 1.
[23] See Williamson Murray and Allan R. Millet, Military Innovation in the Interwar Period (Cambridge: Cambridge University Press, 1996).
[24] See Stephen Peter Rosen, Winning the Next War: Innovation and the Modern Military (Ithaca: Cornell University Press, 1991), 2.
[25] Jon R. Drushal, Additive Manufacturing: Implications to the Army Organic Industrial Base in 2030. Civilian Research Project USAWC Fellow, U.S. Army War College. Carlisle, PA, April 2013.
[26] President Obama started the National Network for Manufacturing Innovation (NNMI), a public-private partnership, over two years ago. The network consists of regional innovation hubs for the development and adoption of cutting-edge manufacturing. The National Additive Manufacturing Institute (NAMII) also called America Makes, is a 2012 pilot specifically focused on accelerating breakthroughs in 3D printing. The Department of Defense leads two institutes focused on "Digital Manufacturing and Design Innovation" and "Lightweight and Modern Metals Manufacturing." For more information see "National Network for Manufacturing Innovation," Advanced Manufacturing Portal, n.d., http://manufacturing.gov/nnmi.html; See also White House, Office of the Press Secretary, "Obama Administration Launches Competition for Three New Manufacturing Institutes," May 9, 2013.
[27] The author thanks her colleagues at the Potomac Institute for Policy Studies, particularly Mike Swetnam, Jennifer Buss, and Patrick Cheetham, for their astute comments about the EC&P.
[28] For a description of the EC&P connection to the ASD(R&E), see Richard Hencke, "Prototyping: Increasing the Pace of Innovation," Defense AT&L, July/August, 2014.

TIME TO DEPLOY CONVENTIONAL PROMPT GLOBAL STRIKE

THOMAS SCHEBER

For more than a decade, the United States has pursued a conventional prompt global strike (CPGS) capability. The development and deployment of CPGS has been endorsed by the administrations of both George W. Bush and Barack Obama. Yet, after more than a decade of development, the Department of Defense (DoD) still has no firm plans to deploy such revolutionary weapons.

All this has generated a pair of questions that jointly have dominated the policy debate on the subject. Namely, what are the prospects for deployment of a CPGS capability in the near term? And how would such a capability serve U.S. interests vis-à-vis potential adversaries?

WHAT IS CPGS

CPGS was defined initially as the ability to strike anywhere in the world with a conventional weapon within an hour after the execution order is given.[1] This unique capability was deemed important to be able to strike high priority, fleeting targets such as terrorist actors, or interrupt the transfer of weapons of mass destruction. At present, the only prompt global strike capability available to a U.S. president is limited to nuclear warheads delivered by ballistic missiles. Given the potential fallout from any such strike, a prompt conventional strike capability could be of significant value and would fill a gap in U.S. military capabilities.

In the past, prompt, very accurate, intercontinental-range conventional weapons were not feasible. The limitations of guidance technology and the lack of timely, precise intelligence foreclosed such developments. Over the past two decades, however, the development of precision guidance technologies, space-based navigation aids, and surveillance capabilities has made possible a variety of long-range, conventional weapons. DoD's current interest in such weapons is the natural progression of military capabilities enabled by advanced technologies in a changing security context.

POTENTIAL BENEFITS AND LIMITATIONS OF CPGS

U.S. defense officials from both political parties have envisioned CPGS as a "niche" strike capability which would be procured in limited quantities—at most, tens of missiles. Such a capability could be of great value in disrupting an ongoing action in distant parts of the world. The damage inflicted by a CPGS weapon may not be catastrophic against some enemy targets, but it could be sufficient to cripple adversary actions until heavier and more sustained strike capabilities and defenses could be moved into place.

The limitations of CPGS have been well documented. The weapons would be expensive, the damage inflicted by CPGS payloads would be limited by weight and volume constraints for ballistic missile payloads, and concern exists over the potential for Russia, or in the future some other country, to mistake a CPGS launch for a nuclear attack. Even so, assessments such as the 2008 study by the National Research Council concluded that CPGS could be of great value and the identified drawbacks were manageable.[2] The potential for timely employment of such a weapon would, of course, be dependent on near-real-time and accurate intelligence. Such intelligence could not be guaranteed, but this is a competency in which the United States excels and adversaries lag far behind.

***Thomas Scheber** is the Vice President of the National Institute of Public Policy based in Fairfax, VA. He served as the Director for Strike Policy and Integration in the Office of the Secretary of Defense from 2003 to 2006.*

POTENTIAL CPGS DEVELOPMENT BY OTHER COUNTRIES

Interest in prompt, conventional weapons of various ranges is not unique to the United States, however. Several countries, including Russia and China, have deployed or are developing such weapons.

Russia

Russia continues to assign highest priority to modernizing its extensive nuclear forces. This is intended to help compensate for the inferiority of its general purpose military capabilities, counter superior U.S. conventional forces, and restore one aspect of its past superpower status. However, Russian military planners have recognized the value of high-precision weaponry as a complement to their nuclear forces in the Twenty-First Century security environment. In fact, Russia's most recent military doctrine, issued in 2014, assigns high-precision conventional weapons to the mission of strategic deterrence.[3]

According to one former Russian official, Russia plans to equip a growing share of strategic delivery systems with conventional warheads.[4] For example, Russia deploys both conventional and nuclear warheads on short-range *Iskander* missiles and is capable of outfitting its newer submarine-launched ballistic missiles with low-yield nuclear warheads or conventional warheads with precision delivery. In December 2012, the Commander of Russia's Strategic Missile Forces, Colonel-General Sergei Karakayev, said that Russia was also considering developing a conventional payload for its new powerful, liquid-fueled ICBM.[5] Subsequently, Russian President Vladimir Putin spoke publicly about the value of "high-precision weapons" for deterrence and asserted that Russia had already started supplying its military with such weapons.[6] In November 2014, a Russian defense industry executive announced that Russia would have an air-launched hypersonic missile by 2020.[7] This interest in acquiring prompt conventional strike capabilities appears to demonstrate that, despite earlier protestations about U.S. CPGS concepts, Russian defense planners understand the political and military utility of such weapons.

China

Since the 1990s, China has been developing and producing conventionally-armed ballistic missiles. According to Chinese sources, Xi Jinping, China's President and Chairman of the Central Military Commission of the Chinese Communist Party, has ordered the People's Liberation Army (PLA) to build a powerful and technologically advanced missile force.[8]

Russia's most recent military doctrine, issued in 2014, assigns high-precision conventional weapons to the mission of strategic defense.

These "conventional missiles for strategic use" are intended primarily to intimidate Taiwan, for use in wars in the western Pacific, and to support China's anti-access/access-denial strategy against the U.S. military. These missiles do not need to be of global reach to support China's strategy of dominating the western Pacific. According to one China analyst, the PLA's conventional prompt ballistic missile inventory includes about 1,200 short-range missiles (DF-11/CSS-7 and DF-15/CSS-6), medium-range missiles such as the DF-21/CSS-5 family which includes an anti-ship version and the DF-16/CSS-11 which can target Okinawa, and development of an intermediate-range missile, the DF-26, which will be able to target U.S. and allied capabilities as distant as Guam.[9] In January 2014, China reportedly tested a hypersonic glide vehicle (HGV) designed to be launched from ICBM missile boosters. The vehicle, dubbed WU-14 by the Pentagon, is described as capable of maneuvering and gliding to its target at speeds up to ten times the speed of sound (i.e., hypersonic). The accuracy and potential military effectiveness of China's conventionally-armed ballistic missiles is not known and, to date, the anti-ship DF-21D has not been tested against a moving target at sea.

Pakistan and India

Pakistan, India, and others already deploy prompt, conventionally-armed missiles. For example, in early 2012, Pakistan test-fired a short-range ballistic missile that was characterized by a Pakistani military spokesman as having "high maneuverability, pinpoint accuracy."[10] The Hatf-II missile, also called the Abdali, is reported to have a range of 180 kilometers and be capable of carrying either a conventional or nuclear warhead. India also has conventionally-armed ballistic missiles. In addition, India's Defense Research and Development Organization (DRDO) has teamed with a Russian weapons firm to develop a hypersonic cruise missile. The missile, referred to as BrahMos, reportedly has a range of about 290 kilometers. A supersonic version of the BrahMos was successfully test fired in December 2008, and further development of a hypersonic version is now underway.

At present, the only prompt global strike capability available to a U.S. president is limited to nuclear warheads delivered by ballistic missiles.

U.S. developments

For the United States, an extensive history of weapon development programs provides the technological foundation to pursue CPGS concepts. Several initiatives, stretching from the late 1970s to the early 2000s, have provided experimental data on which to base further development.

Maneuvering Reentry Vehicles (MaRVs). One U.S. concept for a MaRV, called SWERVE was developed during the Cold War to enable U.S. reentry vehicles and nuclear warheads to evade Soviet defenses. According to a NASA report, the first SWERVE flight test occurred in 1979 and the last in 1985.[11] The SWERVE concept demonstrated the ability to maneuver RVs during reentry by using an asymmetrical nose cone and control of the RV's attitude once in the atmosphere. Precision accuracy, however, was not achievable at intercontinental ranges with 1980s technology.

TACMS-P Concept Demonstration. One DoD Advanced Concept Technology Demonstration (ACTD) Program pursued in the early 2000s was called TACMS-P (also called ATACMS-P). The concept used a short-range ballistic missile to deliver an earth penetrating warhead with conventional explosives and precision accuracy. In 2004, the TACMS-P concept was successfully demonstrated using a 220 kilometer-range missile fired from an Army Multiple Launch Rocket System. The missile carried a Navy-developed reentry vehicle (RV) for precision accuracy. This technology demonstration program concluded in August 2005 with another successful test flight at White Sands Missile Range.

Enhanced Effectiveness Reentry Vehicle (EERV). Also early in the 2000s, the Navy explored fitting an existing RV system with a "backpack" containing a guidance system and maneuvering control flaps. The initial CPGS concept proposed for deployment in 2003 was for a conventionally-armed Trident II/D5 missile based on the EERV concept.

Recent flight test experience. In the past few years, DoD has conducted experimental flight tests of two hypersonic glide vehicle (HGV) concepts. The Advanced Hypersonic Weapon (AHW) being developed by the Army is based on improvements to the SWERVE concept. Another new concept is being jointly developed by the Defense Advanced Research Projects Agency and the Air Force and is referred to as HTV-2. In addition, the Air Force has been experimenting with an air-launched, scramjet, hypersonic missile—the X51A Waverider. In general, flight test results have been mixed, indicating that control and delivery of payloads at hypersonic speeds over intercontinental ranges remains a technology challenge.[12]

Depending on the delivery vehicle and basing mode/location, these weapons could be accountable under the New START Treaty.

IMPLICATIONS FOR U.S. SECURITY

For over two decades, the United States has enjoyed a position of dominance in precision strike technology. The success of the short-range TACMS-P and intercontinental-range EERV programs demonstrates that the technology exists to field a near-ballistic CPGS capability in the near term. Depending on the delivery vehicle and basing mode/location, these weapons could be accountable under the New START Treaty.[13] In fact, after the New START Treaty was signed in 2010, Obama administration officials testified before Congress during the ratification process and indicated that a "few tens of accountable" CPGS weapons would be reasonable.[14] However, for the past several years, the United States has pursued non-ballistic concepts such as HGVs which would not fall under the definitions of weapons limited or prohibited by existing arms control treaties.

The United States has delayed decisions on which initial CPGS concepts are to be deployed while working to advance the most challenging delivery technologies. In a February 2011 report to Congress on CPGS programs, the Obama Administration declared that it had "no plans to develop and field" CPGS concepts based on ballistic missile delivery, and would, instead, develop non-ballistic concepts—such as HGVs—which would not be arms control constrained.[15] Thus, the United States appears to be bypassing the near-term option of deploying relatively mature technologies for CPGS and waiting until more technologically demanding, non-ballistic options—such as the AHW, HTV-2, or Waverider concepts—are available.

Moreover, CPGS development has slowed recently due to shrinking defense budgets, sequestration, and competition for funds among a plethora of DoD programs. Meanwhile, Russia, China, and others continue to demonstrate and advance new technologies for prompt, precision strike.

For the United States, the rationale for CPGS remains as valid as when it was first proposed. The United States has strategic interests in distant parts of the world, and there is no guarantee that general purpose forces could be brought to bear in time should an urgent situation arise. Currently, the United States still commands unique capabilities needed to employ effectively a prompt global strike capability—superb surveillance and intelligence, military forces deployed globally that could provide follow-on strikes (if needed), and the world's best logistic support to enable sustained operations. This advantage should be protected by moving forward soon on deployable CPGS weapons while continuing to invest in more sophisticated, but challenging, delivery technologies.

ENDNOTES

[1] National Research Council Committee on Conventional Prompt Global Strike Capability, U.S. Conventional Prompt Global Strike: Issues for 2008 and Beyond (Washington, DC: National Academies Press, 2008), 21.

[2] Ibid., 4, 10-12, 15, 59-60.

[3] Military Doctrine of the Russian Federation, approved by Russian Federation President V. Putin, December 26, 2014, paragraph 26.

[4] Nikolai Sokov, "The New, 2010 Russian Military Doctrine: The Nuclear Angle," James Martin Center for Nonproliferation Studies, February 5, 2010, http://cns.miis.edu/stories/100205_russian_nuclear_doctrine.htm.

[5] "Russia to Develop Precision Conventional ICBM Option," RIA Novosti, December 14, 2012.

[6] Diane Barnes, "Putin Eyes 'High-Precision' Arms as Partial Nuclear-Weapons Alternative," Global Security Newswire, December 3, 2013.

[7] "Russia Expected to Have Hypersonic Air-Based Missile by 2020," Interfax-AVN, November 13, 2014.

[8] "Xi Jinping Calls for Powerful Missile Force," Xinhua, December 5, 2012, http://news.xinhuanet.com/english/china/2012-12/05/c_132021964.htm.

[9] Richard D. Fisher, Jr., "General Secretary Xi Jinping on Nuclear Weapons, Missiles and Space Warfare," International Assessment and Strategy Center, November 3, 2014, 3, http://www.strategycenter.net/research/pubID.349/pub_detail.asp.

[10] "Pakistan Test-Fires Nuclear Capable Ballistic Missile," Deutch Presse-Agentur, March 5, 2012.

[11] Kenneth W. Iliff and Mary F. Shafer, "A Comparison of Hypersonic Vehicle Flight and Prediction Results," NASA Technical Memorandum 104313, October 1995, 7.

[12] For a more detailed discussion of recent flight tests for CPGS concepts, see Amy F. Woolf, "Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues," Congressional Research Service Report R41464, August 26, 2014.

[13] For a detailed discussion of potential treaty issues associated with CPGS concepts, see Keith Payne, Thomas Scheber, Mark Schneider, David Trachtenberg, and Kurt Guthe, Conventional Prompt Global Strike: A Fresh Perspective (Fairfax, Va.: National Institute Press, June 2012), 29-37.

[14] James N. Miller, Principal Under Secretary of Defense for Policy, in Senate Armed Services Committee, Nuclear Posture Review, S. Hrg. 111-824, 111th Cong., 2d sess. (Washington, DC: GPO, 2011), 33-34.

[15] Barack Obama, "Report on Prompt Global Strike," The White House, February 2, 2011, 2.

"Red World Map" cover art courtesy of Vector Templates

MANUSCRIPTS SHOULD BE SENT TO the attention of the Editor at 509 C Street, NE, Washington, DC 20002, or submitted via email to defensedossier@afpc.org. The Editors will consider all manuscripts received, but assume no responsibility regarding them and will return only materials accompanied by appropriate postage. Facsimile submissions will not be accepted.

EDITOR'S NOTE: The opinions expressed in the Defense Dossier (ISSN 2165-1841) are those of the author(s) alone and do not necessarily represent the opinions of the American Foreign Policy Council.

About the American Foreign Policy Council

For more than three decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

DEFENSE DOSSIER

AMERICAN FOREIGN POLICY COUNCIL

American Foreign Policy Council
509 C Street, NE
Washington, D.C. 20002
www.afpc.org