ISSUEBRIEF   BY **JAMES HASIK** AND **MARK REVOR**

Democratized Destruction: Global Security in the Hacker Era

SEPTEMBER 2014

The democratized innovations of today's Hacker Era have a dark side: democratized destruction, underwritten by advanced information technologies and spread by highly empowered individuals with very undemocratic intent. The breadth, pace, diffusion, and potential for concealment of these advances may be creating new vulnerabilities for the same technologically advanced societies that spawned them. Fortunately, the United States and its allies have experience with this mode of innovation and unique resources for developing countermeasures. We recommend three courses of action: leveraging capital investments with low marginal cost extensions, monitoring the global progress of open innovation, and supporting domestic grassroots developments in information-intensive systems.

The Hacker Era of Democratized Destruction

Rapid, unchecked development in computing and communications technologies is spawning a Hacker Era that gives highly determined and resourceful individuals—and not just powerful governments—access to advanced military technologies.[1] The concept of *democratized innovation*, as developed by Eric von Hippel of the Massachusetts Institute of Technology (MIT), has been most notable in information products and software, particularly regarding open source software. Today, such innovation is occurring not just with original equipment manufacturers (OEMs), or what the defense industry calls "prime contractors," but among users and suppliers. As better tools become available, innovative activity increasingly has been arising

Disrupting Defense

This issue brief serves to further the discussion launched at the Atlantic Council's conference Disrupting Defense: Dynamic Security in an Age of New Technologies. The conference hosted leaders from government, business, media, and think tanks to explore technology's disruptive impact on geopolitics, efforts by public and private investors to fund technological breakthroughs, and the new ways the United States and its allies equip their forces for wars of the future. The Disrupting Defense conference was hosted at Council's Brent Scowcroft Center on International Security by its Strategic Foresight Initiative and its Emerging Defense Challenges Initiative, of which George Lund is the principal sponsor.

wherever the greatest benefit to the potential innovator is found.[2]

With these tools "in the hands of the many, not the few," a dark side to this democratized innovation has emerged, in which some who benefit have highly undemocratic intent.[3] The overwhelming conventional military power of the United States and its allies constrains opponents' options: acquire a nuclear deterrent, innovate technologically, or face defeat.[4] The United States should thus consider two questions:

2   Eric von Hippel, *Democratizing Innovation* (Cambridge, MA: MIT Press, 2005).

3   Comments by Andrew Hoehn, senior vice president for research and analysis at RAND, and Moisés Naím, senior associate, Carnegie Endowment for International Peace, at the Atlantic Council's Disrupting Defense conference, May 14, 2014.

4   August Cole and Ben FitzGerald, "Peering into America's Military Blind Spots: High-Impact Long Shots," *War on the Rocks*, July 3, 2014, http://warontherocks.com/2014/07/peering-into-americas-military-blind-spots-high-impact-long-shots/.

1   Comment by Mathew Burrows, senior fellow at the Atlantic Council, May 14, 2014.

James Hasik is a senior fellow at the Brent Scowcroft Center on International Security at the Atlantic Council. **Lieutenant Colonel Mark Revor** was the 2013–2014 Marine Corps fellow at the Atlantic Council and now serves in the White House Military Office.

First, "how long is it before the worst weapons are in the hands of the worst actors?"[5] And second, what can be done about it?

Five Hallmarks of Democratized Military Technologies

To understand the threat, one should consider the driving factors. James Miller, a former US undersecretary of defense for policy, argues that the Hacker Era has five facets technologically, in breadth, pace, concealment, diffusion, and vulnerabilities.[6]

> THE POTENTIAL FOR THE CONCEALMENT OF DESTRUCTIVE TECHNOLOGIES IS ALSO ACUTE, AS THE HACKER APPROACH COMPRISES IED WORKSHOPS IN GARAGES, HOMEMADE DRONES IN BACKPACKS, BIO-LABORATORIES IN BASEMENTS, AND CYBER WEAPONS ON LAPTOPS.

The breadth of technological change is very wide, affecting areas from biotechnology to additive manufacturing. As von Hippel has observed, many of today's technological advances have information technology at their root, so improvements in computing and communications power have cascaded into advances in a host of fields susceptible to automated design and manufacturing. This recombinant capacity is leading to emergent advances from unexpected avenues. After all, the Internet boom loomed for years with the development of faster processors and bigger bandwidths, but few really grasped the economic possibilities until they suddenly began appearing in the late 1990s.[7]

The pace of change is thus very quick, with competitive developments in some military domains

beginning to follow Moore's Law. The experience with tactical cycle time from the campaign in Afghanistan is instructive. In signals intelligence and in battles against improvised explosive devices (IEDs), Coalition troops initially used old jamming devices that, although generally effective, could be decoded by a technologically adept insurgent using commercially available frequency-scanning devices. The insurgents responded by using frequency-coding devices for radio triggers, low-metallic casings for avoiding detection, and vehicle traffic pattern analysis for finding targets.[8] In this context, the struggle is now fought on thirty-day cycles between the insurgents' latest weapons, the coalition's countermeasures, and the insurgents' next design and manufacturing efforts. And cyber conflict is shaping up to be an even faster fight, as software techniques can be altered within days.[9]

The potential for the concealment of destructive technologies is also acute, as the hacker approach comprises IED workshops in garages, homemade drones in backpacks, bio-laboratories in basements, and cyber weapons on laptops.[10] Small, sophisticated, factory-built weaponry has become more widely available too. IEDs have been the insurgents' artillery in Iraq and Afghanistan and, eventually, their "weapons of strategic influence."[11] But almost contemporaneously, Hezbollah used proper antitank missiles as their artillery against the Israelis in Lebanon. Wider employment of such portable precision weaponry "could radically intensify the challenges confronting US forces"—consider what Hamas might accomplish with GPS guidance on its rockets.[12] Even human tools like commandos have taken on new power when networked over large areas: the "little green men" of Russia's Spetsnaz took over the whole of Crimea without a shot—much less a badge or a flag. In a potential limited war with NATO, these special forces could be very dangerous even before the actual shooting broke out.[13]

---

5   Comment by Congressman Randy Forbes, "The Congressional Role in US Military Innovation: Preparing the Pentagon for the Warfighting Regimes of Tomorrow," Brookings Institution, Washington DC, July 24, 2014, http://www.brookings.edu/events/2014/07/24-congress-and-military-innovation.

6   Comments at the Atlantic Council's Disrupting Defense conference, Washington DC, May 14, 2014, http://www.atlanticcouncil.org/events/upcoming-events/detail/disrupting-defense.

7   John Alic, *Trillions for Military Technology: How the Pentagon Innovates and Why It Costs So Much* (New York: Palgrave, 2007), chapter 7.

8   Ed Toy, *Pressure Plate: A Perspective on Counter IED Operations in Southern Afghanistan, 2008–2009* (Ex Libris, 2013), pp. 16, 30, 94, 100.

9   Comments by General (ret.) James Cartwright USMC, at the Disrupting Defense conference, May 14, 2014.

10   Comments by Burrows and Naím at the Disrupting Defense conference, May 14, 2014.

11   General Montgomery Meigs, annual report of the Joint IED Defeat Organization (JIEDDO), 2006; and Lt. General Thomas Metz, annual report of the JIEDDO, 2007.

12   David Johnson, *Hard Fighting: Israel in Lebanon and Gaza* (Santa Monica: RAND, 2011), p. xv.

13   Robert Farley, "Five Russian Weapons of War NATO Should Fear," *National Interest*, July 6, 2014, http://nationalinterest.org/feature/five-russian-weapons-war-nato-should-fear-10816.

The rapid and global unchecked diffusion of these technologies and techniques is making those developments accessible to smaller actors. Years ago, different insurgent groups were sharing information through an informal "international business model, with weapons tested in Sri Lanka, engineered in the Balkans, retested in Indonesia, and finally aimed at troops in Afghanistan."[14] The process has been an insurgents' analog to the commercial concept of *open innovation*, as described by Henry Chesbrough of the University of California at Berkeley, in which businesses in multiple industries collaborate in research efforts for common benefit.[15] Many emerging technologies—whether commercial or military in origin—can be manipulated by their end-users, and are thus not under the sole control of well-funded military forces and their suppliers.

> BROAD, FAST-PACED TECHNOLOGICAL CHANGE IS DIFFUSING READILY CONCEALABLE, POWERFUL WEAPONS AROUND THE WORLD TO THE DETRIMENT OF US LEADERSHIP OF THE GLOBAL ORDER. FORTUNATELY, THE UNITED STATES AND ITS ALLIES KNOW HOW TO PLAY THIS GAME AS WELL.

All of this may be creating new vulnerabilities in the global infrastructure of finance, communications networks, supply chains, and travel—hinting that perhaps even the United States' global military-industrial dominance may be at risk. As Harvard University's Clay Christensen has argued, "transformational shifts within industries often take root at the lower end of the market, [and] IEDs and cyber warfare are relatively low-cost technology disrupters."[16]

The American Experience

The model described here may sound dystopian: broad, fast-paced technological change is diffusing readily concealable, powerful weapons around the world to the detriment of US leadership of the global order. Fortunately, the United States and its allies know how to play this game as well. As RAND's Adam Grissom has shown, what experts may now call democratized innovation has had a long history.[17] This "bottom-up" approach has famously been the German way: fueled by the *auftragstaktik* of the prewar years, the development of the *Strumtruppen* in the First World War began with a captain on the Western Front.[18] A decade later, it became the Marine Corps way, in learning how to fight the small wars of the interwar years.[19] Even the rather hierarchical US Air Force had early experience with user innovation: its rapid development of close air support tactics in 1944 was led by Major General Elwood Quesada, but it was substantially a squadron-level process.[20] In 1962, John Boyd and Tom Christie famously and illicitly borrowed time on an IBM 704 to work out the details of Energy-Maneuverability Theory.[21] The Navy's classic story is that of the lieutenant at the Submarine School who developed the eponymous Ekelund range formula and circular slide rule—still used in updated electronic form around the world.[22] Bottom-up innovation may not have always been the US Army way, in the "Big Army" way of thinking in the Cold War, but it became more ingrained during the Iraq war with the entrepreneurial launch of social networking tools such as CompanyCommander.com.[23]

14   Mike Aldrich and James Hasik, *Arms and Innovation: Entrepreneurship and Alliances in the Twenty-First Century Defense Industry* (Chicago: University of Chicago Press, 2008), p. 134.

15   Henry Chesbrough, *Open Innovation: The New Imperative for Creating and Profiting from Technology* (Boston: Harvard Business School Press, 2003).

16   William Lynn and James Stavridis, "Commentary: Creative Disruption on Horizon," *Defense News*, July 7, 2014, http://www.defensenews.com/article/20140707/DEFFEAT05/307070013/Commentary-Creative-Disruption-Horizon.

17   Adam Grissom, "The Future of Military Innovation Studies," *Journal of Strategic Studies*, vol. 29, no. 5, October 2006, pp. 905–934.

18   Timothy T. Lupfer, *The Dynamics of Doctrine: The Change in German Tactical Doctrine During the First World War*, Leavenworth Paper #4, Combat Studies Institute, US Army Command & General Staff College, July 1981; Bruce I. Gudmundsson, *Stormtroop Tactics: Innovation in the German Army, 1914-1918* (Westport: Praeger, 1995).

19   Keith B. Bickell, *Marine Learning: The Marine Corps Development of Small Wars Doctrine, 1915–1940* (Boulder: Westview, 2000).

20   Thomas A. Hughes, *Overlord: General Pete Quesada and the Triumph of Tactical Air Power in World War II* (New York: Free Press, 1995).

21   Robert Coram, *Boyd: the Fighter Pilot Who Change the Art of War* (Boston: Little, Brown & Company, 2002), pp. 135–153.

22   Michael Foutch, "The Ekelund Range," *Undersea Warfare*, vol. 4, no. 2, winter/spring 2002.

23   Janine Davidson, *Lifting the Fog of Peace: How Americans Learned to Fight Modern War* (Ann Arbor: University of Michigan Press, 2010), p 202.

Demonstrators in Berlin protested the controversial US surveillance program PRISM during Barack Obama's October 2013 visit. *Source*: Mike Herbst (licensed under Creative Commons).

It was certainly helpful that the recent generation of junior officers grew up in the 1990s, when computing technologies were already part of daily life. FalconView, the USAF's desktop computer mission planning system, provides an excellent and recent example of this acceleration of innovation by electronic tools. The system's first forerunner, FPLAN, was largely written by two A-10 pilots in 1981 on a TRS-80. The next development, ODD, was written by two Utah Air National Guard F-16 pilots in the late 1980s. The release of Windows 3.0 in 1991 immensely helped: one of the officers who wrote ODD teamed up with some engineers at the Georgia Tech Research Institute to create the much more user-friendly FalconView. For several years thereafter, the tool was popular, but not universally adopted. In 1996, the crash of then-Commerce Secretary Ron Brown's transport at Dubrovnik, Croatia, provided the impetus for change: the accident investigation board concluded that FalconView in the cockpit would have saved all thirty-five aboard. The application was taken up widely and rapidly, and thereafter significantly extended by a group of officers with good programming skills. In a now-classic maneuver, FalconView became a freely available, open-source

project in 2009.[24] In a sign of its success, many of FalconView's software components have been incorporated into the Joint Mission Planning System, now mandated for use across all the military services.

Limits to the Democratic Model

One might worry that enemies around the world have thousands of their own determined hackers that are launching hundreds of their own projects, more lethal than mere mission-planning software. Fortunately, competition is not just a matter of keeping up, for two restraining factors may limit the damage.

First, war in the premier league is a capital-intensive business. The interplay of technology and finance is an important determinant: with limited funds, users can more readily write code than bend steel. However highly motivated toward deck-plate solutions, deck officers generally cannot build their own ships. Backpack drones with line-of-sight links cannot accomplish what Reapers do with satellite links.[25] This problem affects even the United States: the "farmer armor" meant to fend off IEDs in Iraq was

---

24 Jon R. Lindsay, "War upon the Map: User Innovation in American Military Software," *Technology and Culture*, vol. 51, no. 3, July 2010, pp. 619–651.
25 Lynn E. Davis et al., *Armed and Dangerous? UAVs and US Security* (Santa Monica: RAND, 2014).

never professional grade, whatever the impetus for field-level learning and experimentation.[26]

Thus, the second point—even a groundswell of enthusiasm is sometimes insufficient for lasting innovation.[27] Thirty-five deaths led the Air Force to distribute widely the inexpensive FalconView, but thousands of fatalities from IEDs were needed before the Army and the Marine Corps procured thousands of million-dollar MRAPs.[28] If the IEDs of Iraq and Afghanistan are harbingers of future conflict, then they are a forgettable experience that must not be forgotten. The foremost lesson, though, is not that the US military struggled to find technical solutions to the threat, but that it did not adapt conceptually and culturally for a fight it had not anticipated.[29] The forces were hamstrung by bureaucratic predispositions toward big projects with top-down control, even in such fast-moving fields as enterprise software.[30] For in government procurement, where money is power, few want to be in charge of something small.[31]

Low Marginal Costs, a Weather Eye, and Well-Funded Geeks

So, amid this history of threats, successes, and limitations in this model of democratized destruction, what can be done? To address the darker possibilities of the Hacker Era, the United States must consider three approaches: one to counter the tide and two to surf ahead of it:

Find capital-intensive but low marginal-cost solutions to "democratized" threats. The American way of war has traditionally relied on capital-intensive attrition, but in the precision era, expensive defenses work against

THIRTY-FIVE DEATHS LED THE AIR FORCE TO DISTRIBUTE WIDELY THE INEXPENSIVE FALCONVIEW, BUT THOUSANDS OF FATALITIES FROM IEDS WERE NEEDED BEFORE THE ARMY AND THE MARINE CORPS PROCURED THOUSANDS OF MILLION-DOLLAR MRAPS.

swarming attackers only until the magazines empty out.[32] Energy weapons, though, continue to work long *after* the other side's magazines empty out. Broadly speaking, lasers, rail guns, and cyberweapons are in a class of potentially disruptive technologies that democratized destructiveness cannot address. Another approach comprises methods of autonomy from remote piloting to distance learning. Consider how, over the lifecycle of most manned aircraft, 50 percent of operations and maintenance costs can be attributed to aircrew training.[33] For a late model F-16 fighter jet, that comes to $7,500 per flight hour—in contrast to the a few hundred per simulator hour for training drone pilots.[34] And while virtual presence may be actual absence, these tools of what James Cartwright has termed *cognitive mobility* provide great leverage to large and sunk investments in war-fighting kit.[35] For if the enemy can only afford local, distributed solutions, the efficient response may be an asymmetrically capital-intensive assault on the enemy's grassroots tools.

Monitor the global progress of open innovation. As with IEDs, the first to develop a technology is often not the

26 John Barry and Babak Dehghanpisheh, "Hillbilly Armor," *Newsweek*, December 19, 2004; and James Hasik, "Professional Grade: A Working Paper on Recent Fatalities in Military Vehicles in Iraq and Afghanistan," October 2006, http://www.slideshare.net/jhasik/professional-grade.

27 Terry C. Pierce, *Warfighting and Disruptive Technologies: Disguising Innovation* (London: Frank Cass, 2004), p. 3. See also James Hasik and Byron Callan, "Disrupt or Be Disrupted: How Governments Can Develop Decisive Military Technologies," Atlantic Council, May 2014, http://www.atlanticcouncil.org/images/publications/Disrupt_or_Be_Disrupted.pdf.

28 All the same, the cost effectiveness of MRAPs, in relation to the value of statistical life, has been disputed. See Christopher Rohlfs and Ryan Sullivan, "The Cost-Effectiveness of Armored Tactical Wheeled Vehicles for Overseas US Army Operations," *Defence and Peace Economics*, vol. 24, no. 4, pp. 293-316, and the ensuing debate in issue no. 5.

29 Cartwright, May 14, 2014.

30 Michael Grothaus, "Why Exactly Does the Government Suck So Badly at Software?" *Fast Company*, May 27, 2014, http://www.fastcolabs.com/3031108/why-exactly-does-the-government-suck-so-badly-at-software.

31 "How to Ignite Innovation," interview with Lt. Col. Dan Ward USAF, *Defense News with Vago Muradian* video, July 6, 2014, http://www.defensenews.com/VideoNetwork/3655731257001/How-to-Ignite-Innovation.

32 Russell F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (Bloomington: Indiana University Press, 1977); Michael Russell Rip and James Hasik, *The Precision Revolution: GPS and the Future of Aerial Warfare* (Annapolis: Naval Institute Press, 2002), chapter 13.

33 Cartwright, May 14, 2014.

34 Maj. Gen. James Jones, Air Force assistant deputy chief of staff for operations, plans and requirements, at the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC), Orlando, December 3, 2013; See Aaron Mehta, "Under Budget Pressure, US Air Force Looks to LVC Training," *Defense News*, May 20, 2014.

35 The phrase "virtual presence is actual absence" has become popular, but perhaps the first mention was by Admiral Mike Mullen at the National Defense University, Fort McNair, Washington DC, August 16, 2005, http://www.navy.mil/navydata/cno/mullen/speeches/mullen050816.txt.

first to employ it in a truly disruptive manner.[36] The United States has been largely leading the way with drone aircraft, but the first true outdoor swarming—or flocking—was recently demonstrated by a Hungarian team researching bird behavior.[37] The low cost of entry for research and transnational collaboration in many information-intensive fields means that advances can come from anywhere, and a rash of such competitive developments from China to Israel have evoked assertions that the United States falling behind in robotics.[38] So while James Miller usefully institutionalized a Defense "red team" for operational planning, another for technological and industrial developments is warranted.[39] Fortunately, the Pentagon is in the process of establishing a formal international research and development tracking function.[40]

> ## IN THE UNITED STATES, RAPID INNOVATION NEEDS A MORE DIRECT, OPEN, AND DEMOCRATIZED PATH FROM FRESH THINKING TO FRUITION.

Provide seed funding and resources to military user-innovators. Finally, while "our geeks" are likely better than their geeks, ISIS and the others lack the burden of a JCIDS process.[41] While scale and scope economies are an American comparative advantage, in the words of Defense Advanced Research Projects Agency (DARPA) Director Arati Prabhaker, the pure pursuit of complex, monolithic systems "is now killing us."[42] In the United States, rapid innovation needs a more direct, open, and democratized path from fresh thinking to fruition. Self-organized activities like the Defense Entrepreneurs Forum (DEF) show that junior officers and noncommissioned officers are keen to innovate on their own, with or without blessings from above.[43] All the same, they could bear such help. As they tap into emerging tools of innovation, they could use a fraction of the funding and bureaucratic resources accorded large-scale contractor-led projects. For every F-22, the United States could use a few FalconViews.[44]

42 George Leopold, "DARPA Chief: Military's Focus on Big Systems 'Is Now killing Us,'" *Defense Systems*, July 29, 2014.

43 Von Hippel (2005) also discusses the importance of open collaboration in chapter 10. This year's DEF is scheduled for October 24-26 at the University of Chicago's Booth School of Business.

44 Richard Danzig, *Driving in the Dark: Ten Propositions about Prediction and National Security* (Washington, DC: Center for a New American Security, October 2011), pp. 21–23.

36 James Hasik and Byron Callan, "Disrupt or Be Disrupted: How Governments Can Develop Decisive Military Technologies," Atlantic Council, May 2014.

37 Ed Yong, "Autonomous Drones Flock Like Birds," *Nature*, February 26, 2014.

38 Michael C. Horowitz, "The Looming Robotics Gap," *Foreign Policy*, May 5, 2014, http://www.foreignpolicy.com/articles/2014/05/05/the_looming_ robotics_gap_us_military_technology_dominance; Paul Scharre, "How to Lose the Robotics Revolution," *War on the Rocks*, July 29, 2014, http:// warontherocks.com/2014/07/how-to-lose-the-robotics-revolution/.

39 Dave Dilegge, "Dr. James Miller: Pentagon's Loss Another's Gain," *Small Wars Journal*, November 8, 2013.

40 Zachary Fryer-Biggs, "International Partners Key to DoD's New R&D Strategy," *Defense News*, July 7, 2014, http://www.defensenews.com/ article/20140707/DEFREG02/307070008/International-Partners-Key-DoD-s-New-R-D-Strategy.

41 Joint Capabilities Integration Development System. See Michael Hoffman, "Outgoing U.S. ISR Chief Slams Slow Acquisition," *Defense News*, August 16, 2010, p. 28; James Hasik, "'Al Qaeda Doesn't Have a JCIDS Process'— Thoughts on Institutionalizing Rapid Acquisition," paper at the first annual Boyd & Beyond Symposium, Marine Corps University, Quantico, Virginia, October 15, 2010.

Atlantic Council Board of Directors