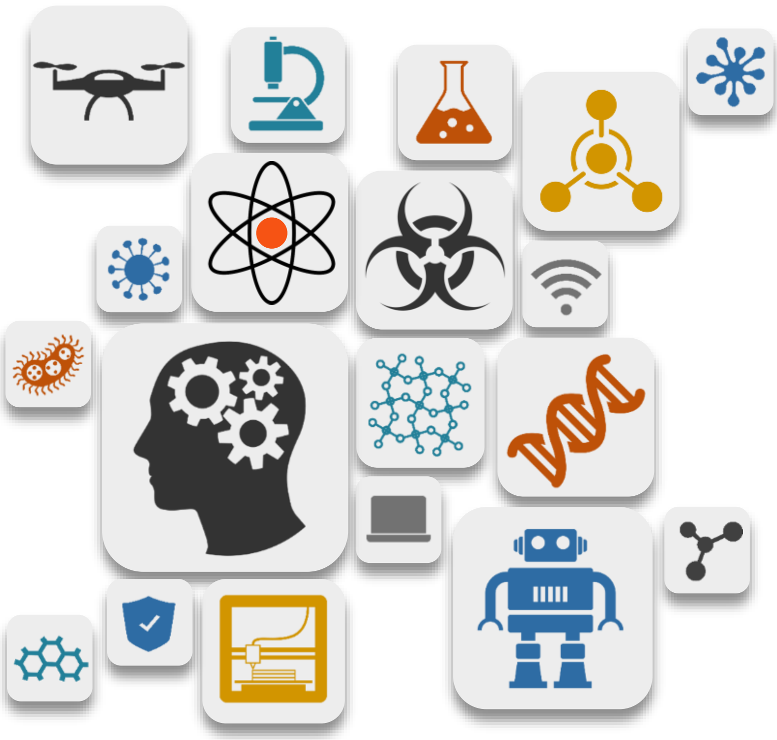
Peril and Promise

Emerging Technologies and WMD

Natasha E. Bajema and Diane DiEuliis



Center for the Study of WMD Weapons of Mass Destruction

Emergence and Convergence
Workshop Report
13–14 October 2016

National Defense University

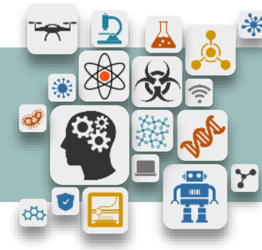
Center for the Study of Weapons of Mass Destruction
National Defense University

MR. CHARLES LUTES
Director

MR. JOHN P. CAVES, JR.
Deputy Director, Distinguished Research Fellow

Since its inception in 1994, the Center for the Study of Weapons of Mass Destruction (WMD Center) has been at the forefront of research on the implications of weapons of mass destruction for U.S. security. Originally focusing on threats to the military, the WMD Center now also applies its expertise and body of research to the challenges of homeland security. The center's mandate includes research, education, and outreach. Research focuses on understanding the security challenges posed by WMD and on fashioning effective responses thereto. The Chairman of the Joint Chiefs of Staff has designated the center as the focal point for WMD education in the joint professional military education system. Education programs, including its courses on countering WMD and consequence management, enhance awareness in the next generation of military and civilian leaders of the WMD threat as it relates to defense and homeland security policy, programs, technology, and operations. As a part of its broad outreach efforts, the WMD Center hosts annual symposia on key issues, bringing together leaders and experts from the government and private sectors. Visit the center online at http://wmdcenter.ndu.edu/.

Cover Design: Natasha, E. Bajema, PhD, Senior Research Fellow



PERIL AND PROMISE

Emerging Technologies and WMD

Emergence and Convergence
Workshop Report
13–14 October 2016

Natasha E. Bajema, PhD and Diane DiEuliis, PhD

National Defense University Press
Washington, D.C.
May 2017

Opinions, conclusions, and recommendations expressed or implied within are solely those of the contributors and do not necessarily represent the views of the Defense Department or any other agency of the Federal Government.

Portions of this work may be quoted or reprinted without permission, provided that a standard source credit line is included. NDU Press would appreciate a courtesy copy of reprints or reviews.

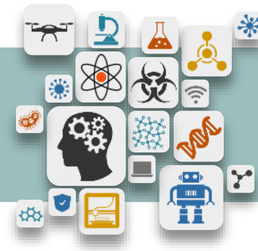


Table of Contents

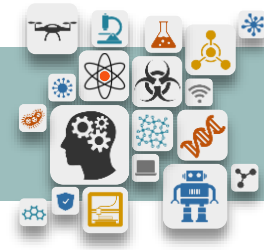
Acknowledgments

The Emergence and Convergence study is supported by several offices within the Office of Secretary of Defense (OSD) including Countering WMD Policy (OSD–Policy) and Threat Reduction and Arms Control (OSD–AT&L). We are thankful to many of our colleagues who provided expertise that greatly assisted the research supporting this report, although they may not agree with all of the interpretations provided in this paper. In particular, we thank the speakers who gave of their time and expertise at the Emergence and Convergence Workshop on 13–14 October 2016, provided comments on this report, and shared their wisdom with us during the course of this research.

We are also immensely grateful to all of the subject matter experts who have volunteered to take the Emergence and Convergence Survey, which, when completed in 2017, will provide invaluable insights on both the risks and opportunities associated with emerging technologies for the WMD space. We acknowledge the incredible work on administering the survey provided by Ken Turner, Intern at the WMD Center. Without his assistance, there would be no survey. Thank you to Mikaela Sparks, Intern at the WMD Center, for her assistance in the editing process.

Finally, we thank Mr. John Caves and Dr. Seth Carus for their comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed professionals.

Introduction



Emerging technologies are transforming life, industry, and the global economy in positive ways, but they also have significant potential for subversion by states and nonstate actors. National security experts, lawmakers, and policymakers have become increasingly concerned about the interactions among a number of emerging technologies that could alter and increase the threats from weapons of mass destruction (WMD).[1]

Emerging technologies are best understood as science-based innovations. Each technology discussed in this paper has the potential to create a new industry or transform an existing one.[2] An emerging technology can arise as an entirely new technology or have a more incremental character, resulting from an existing technology or the convergence of several existing technologies.[3]

Convergence refers to the synergistic integration of new technologies, each of which advances at a rapid rate and interacts with more established fields.[4] Converging technologies interact with other technologies and enable each other in the pursuit of a common goal.[5] Critical convergences among emerging technologies are often dynamic, reinforcing, and/or abridging, providing synergistic effects. Convergences may offer societal benefits, but could also lead to unexpected consequences for national security and the WMD space.

Many emerging technologies have an indirect impact on the WMD space, but only a handful are likely to have direct enabling effects for state and nonstate actors seeking WMD. Such technologies are expected to have serious effects on both the nature of the WMD challenges faced by policymakers and options for countering WMD. Emerging technologies may create new WMD development pathways and/or enhance access to existing ones, leading to increased capabilities of state and nonstate actors to develop and use WMD. Moreover, these technologies might one day lead to a meaningful paradigm shift in how policymakers define WMD, view the threat of WMD, and counter WMD in the future.

To assess the impact of various emerging technologies, it is important to understand how they may be game-changers for state and nonstate actors actively seeking to develop WMD and for policymakers attempting to prevent the proliferation and the use of WMD. Policymakers with responsibilities for countering WMD need answers to the following questions:

- What are the national security risks posed by emerging technologies? What are their enabling effects for the WMD space?
- What new opportunities or solutions do these emerging technologies offer to national security problems and/or the challenge of countering WMD?
- How will these emerging technologies impact traditional tools and approaches for countering WMD? What new types of governance do we need to mitigate the risks?

In its multi-year study entitled *Emergence and Convergence,* the WMD Center will explore the risks, opportunities, and governance challenges for countering WMD introduced by a diverse range of emerging technologies. Toward this end, the WMD Center has developed an exploratory framework for first identifying the emerging technologies that will have greatest impact on the WMD space for state and nonstate actors and then for evaluating the nature of that impact on current tools and approaches for countering WMD. The study uses and adapts the decision framework for managing the risks of dual-use technologies developed by the late Dr. Jonathan Tucker, which assesses technologies for their risk of misuse and governability.[6]

As the first step, the WMD Center identified a list of broad groups of emerging technologies expected to have the greatest impact on the WMD space:

- Additive Manufacturing
- Advanced Robotics
- Nanotechnology
- Nuclear Technology
- Synthetic Biology.

In the second step, the WMD Center will assess these emerging technologies for their risk of misuse and their governability. The risk assessment will include evaluation of near-term capabilities of state and nonstate actors for using specific emerging technologies to develop or deliver WMD within the next 5 years.

In the third step, the WMD Center will evaluate the impact of emerging technologies on current tools and approaches for countering WMD and explore the range of governance options for closing critical gaps. The risk assessment will help to inform priorities and develop and compare different courses of action for addressing any gaps in countering WMD.

Over the next few years, the WMD Center will be using a variety of complementary research methods to explore these critical issues:

- Subject matter expert (SME) risk assessment survey using the Delphi method
- Annual workshop that brings SMEs together with policymakers to discuss risks, opportunities, and governance challenges
- Deep dives on specific issues of concern to the countering WMD policymaking community
- One-on-one interviews with SMEs
- In-depth research on latest trends and developments in emerging technologies.

The study will conclude with a report on its findings, a menu of options for addressing the risks and opportunities produced by emerging technologies for the WMD space, and specific recommendations to policymakers for getting the most return on investment across the menu of options.

---

[1] In this study, WMD refer to traditional CBRN weapons and new weapons with similar effects. For further discussion on definitions, see W. Seth Carus, *Defining "Weapons of Mass Destruction,"* Occasional Paper No. 8, (Washington, DC: NDU Press, 2012), <http://ndupress.ndu.edu/Portals/68/Document

s/occasional/cswmd/CSWMD_OccationalPaper-8.pdf>.

[2] George S. Day, Paul J.H. Schoemaker, and Robert E. Gunther, *Wharton on Managing Emerging Technologies* (New York: Wiley, 2000).

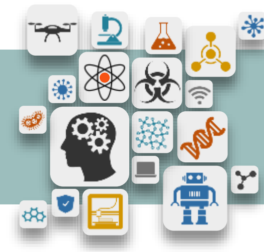
[3] Raji Srinivasan, "Sources, Characteristics and Effects of Emerging Technologies," *Industrial Marketing Management* 37 (2008): 634, <http://www.jotmi.org/index.php/GT/article/view/art400/863>.

[4] Mihail C. Roco, "Possibilities for Global Governance of Converging Technologies," *Journal of Nanoparticle Research: An Interdisciplinary Forum for Nanoscale Science and Technology* 10, no. 1 (2008): 12, doi: 10.1007/s11051-007-9269-8.

[5] Alfred Nordmann, *Converging Technologies: Shaping the Future of European Societies*, Report of the High Level Expert Group on Foresighting the New Technology Wave (Luxembourg: Office for Official Publications of the European Communities, 2004), 14, <http://nanotech.law.asu.edu/Documents/2009/09/final_report_en_243_5158.pdf>.

[6] Jonathan Tucker, ed., *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies* (Cambridge, MA: The MIT Press, 2012).

Workshop and Survey



On 13–14 October 2016, the WMD hosted a workshop at the National Defense University to explore the risks, opportunities, and governance challenges for the WMD space caused by emerging technologies—in particular, additive manufacturing, advanced robotics, nanotechnology, nuclear technology, and synthetic biology. About 100 participants from government, academia, industry, and the nonprofit sector took part in the workshop over the 2 days. The workshop was hosted under NDU's policy of nonattribution, in which remarks are not attributed to speakers or participants without their express permission. This section provides a summary of the proceedings followed by a more in-depth treatment of the discussion for each technology group.

Mr. Chuck Lutes, Director of the WMD Center, opened the workshop by highlighting the challenge of technological forecasting and discussing the WMD Center's broader approach to the Future of WMD 2.0. From 2012 to 2014, the WMD Center undertook a study entitled *WMD Futures* to forecast developments for the WMD space. The study examined, inter alia, a number of emerging technologies—information technology, biotechnology, nanotechnology, advanced energy systems and energetic materials, additive manufacturing, and geophysical weapons—and evaluated their potential for creating "new kinds" of WMD. Several of the WMD Center's current efforts build upon the findings of the study:

- **Emerging Biotechnology**: An ongoing series of deep-dive activities that bring the community of interest together to discuss the risks posed by advances in biotechnology and options for mitigating the risks
- **Cyber Nexus Project**: A one-year investigation of the relationship of cyber to WMD
- **Emergence and Convergence**: A multi-year study that takes a holistic look across relevant emerging technologies to identify priorities for policy intervention.

Together, these research efforts will help to inform policymakers with responsibilities in countering WMD and guide their decisionmaking.

Dr. Natasha Bajema, Senior Research Fellow at the WMD Center, provided a preview of preliminary results from the Delphi method subject matter expert survey. The Delphi method is a structured technique for eliciting expert opinion that was developed by RAND in the 1960s, and it has become an important tool for forecasting the potential risks of new technologies. The method involves a series of iterative questionnaires designed to build an expert consensus on a topic for which there is little or no existing data.

An invitation to participate in the survey was sent to about 3,500 subject matter experts across the Department of Defense, the interagency, academia, industry, and think tanks. The first round of the survey closed on 31 December 2016 with 120 completed responses.

Delphi studies typically involve a small number of targeted respondents and are not intended to produce statistically significant results or predict the response of a larger population. Once concluded, the survey will provide insights derived from the collective wisdom of an informed community on the risks and opportunities posed by emerging technologies for the WMD space.

The major portion of the workshop consisted of five technology panels. These addressed additive manufacturing, emerging biotechnology, advanced robotics, nuclear technology, and nanotechnology. Each panel featured subject matter experts on the risks, opportunities, and governance challenges of emerging technologies.

Dr. Natasha Bajema, Senior Research Fellow at the WMD Center, chaired the first panel on additive manufacturing. **Dr. Tom Campbell**, Office of the Director of National Intelligence, provided a big-picture overview of the national security challenges of 3D printing. **Dr. Bruce Goodwin**, Lawrence Livermore National Laboratory, discussed specific applications of 3D printing for the nuclear industry. **Ms. Anne Kusterbeck**, U.S. Naval Research Laboratory, highlighted the convergence between 3D printing and biotechnology. Concluding the panel, **Mr. Michael Rithmire**, Bureau of Industry and Security at the Department of Commerce, spoke to the challenges of 3D printing for export controls and governance.

Dr. Diane DiEuliis, Senior Research Fellow at the WMD Center, chaired the second panel on emerging biotechnology. **Dr. Megan Palmer**, Stanford University, provided an overview of industry trends in biotechnology and the security implications of new developments. **Dr. Brian Pate**, Defense Threat Reduction Agency, discussed the prospects of bioengineering for defense against WMD. **Dr. Eleonore Pauwels**, Woodrow Wilson Center, spoke to the challenges of governing the fast-moving and complex field of biotechnology. Concluding the panel, **Dr. Sarah Carter**, Science Policy Consulting LLC, highlighted lessons learned from existing policy instruments for biotechnology.

Dr. R.E. Burnett, Associate Dean of Academics of the College of International Security Affairs at NDU, chaired the final panel of the first day on advanced robotics and began by outlining the big picture. **Dr. T.X. Hammes**, Institute for National Strategic Studies (INSS), discussed how small systems such as commercial drones pose a significant threat to national security. **Mr. Mark Colgan**, U.S. Army Edgewood Chemical Biological Center, highlighted the potential of unmanned aerial vehicles (UAVs) and other robotics for countering WMD. Concluding the panel, **Maj Gen Marke "Hoot" Gibson**, USAF (Ret.), Federal Aviation Administration, talked about the governance challenges for countering threats posed by UAVs.

Dr. Tristan Volpe, Carnegie Endowment for International Peace, kicked off the second day by chairing the panel on nuclear technology. **Dr. Edwin Lyman**, Union of Concerned Scientists, provided an overview of trends in the nuclear industry and proliferation risk. **Dr. Ryan Snyder**, Princeton University, discussed the risks associated with laser enrichment technology. **Dr. Wayne King**, Lawrence Livermore National Laboratory, highlighted the ways in which the nuclear industry is harnessing the potential of 3D printing. Concluding the panel, **Dr. James Acton**, Carnegie Endowment for International

Peace, analyzed the different strategies for managing the risks associated with nuclear technology.

Ms. Joanna Gabryszewski, Senior Research Fellow at the WMD Center, chaired the last technology panel on nanotechnology. **Dr. Donna Dulo**, Naval Postgraduate School, provided an overview of nanotechnology and its relevance for WMD. **Dr. Andrew Maynard**, Arizona State University, highlighted the enabling features of nanotechnology. Concluding the panel, **Dr. Michael Meador**, National Nanotechnology Coordination Office, discussed recent efforts to manage the risks and opportunities of nanotechnology.

The workshop concluded with a moderated discussion on the challenges and implications for governance led by **Mr. Chuck Lutes**, Director of the WMD Center. **Dr. Gerald Epstein**, Office of Science and Technology Policy at the White House, began the discussion by outlining different approaches to governance. **Dr. Amy Nelson**, Stimson Center, outlined general challenges to the governance of emerging technology.

Additive Manufacturing

Additive manufacturing creates both new risks and opportunities for the WMD space as a digital manufacturing process, enabling states and nonstate actors interested in WMD with new capabilities. Given the impressive range of manufacturing benefits offered by 3D printing, defense communities will also be able to exploit the technology to develop new solutions to counter WMD and enhance operations in hazardous environments.

Technology Overview

Additive manufacturing, more commonly known as 3D printing, refers to a manufacturing process first developed in the 1980s. The term "additive" refers to a growing family of technologies through which material is added gradually, layer by layer (printed), to build up a 3D object. Every print begins via one of two pathways.

The first pathway starts with a digital 3D blueprint. A 3D model is developed using modeling software such as computer-aided design (CAD) software or purchased and downloaded. The 3D model is then converted to an "STL" file or digital blueprint using "slicing" software, which divides the three-dimensional model into horizontal cross-sections of varying thickness that can be printed sequentially.

The second path begins with any three-dimensional object. A 3D model is produced by scanning an existing object and creating a digital model. The digital model can be modified using modeling software and converted into an STL file.

To perform a print, the 3D printer reads the digital 3D blueprint, lays down successive layers of material, and builds the object. It is worth noting that scanning does not capture the mechanical functionality of the object. For a complex object, each part would have to be separately scanned and assembled to achieve full functionality. Nonetheless, with some skill, the pathway can be used to reverse-engineer existing parts or items.

In recent years, engineers have developed new 3D printing techniques at breathtaking speed, all of which apply the same conceptual process, but use different material types and forms and different printing methods for adding and fusing layers to build objects. Although plastic is the most common material used in 3D printing, a wide range of materials or "inks" are being used in commercial and scientific sectors including plastics, resin, metals (steel, aluminum, bronze, copper, titanium, gold, and silver), ceramics, living tissue, chemical compounds, and nanomaterials.

In 2012, 3D printing overcame nearly two decades of relative obscurity to hit the mainstream with a plethora of media articles appearing in newspapers such as *The Economist*, *New York Times*, and *Wall Street Journal* and a wide range of technical journals. Referred to as "manufacturing for the masses," 3D printing provides broad access to the means of production due to the low capital investment needed to get involved. With just a computer, 3D printer, scanner, and design software, a consumer can design his or her own product on the computer or scan an existing object, purchase and modify a digital product design, distribute the product designs via the Internet and/or print finished products, and sell them online or elsewhere.

By 2020, the market for 3D printers and software is expected to exceed $20 billion.[7] The rise of 3D printing will lead to many economic benefits for the United States including the ability to create complex designs and mass customization and achieve cost savings on materials and distribution and transportation. In the future, manufacturing will be located closer to customers in smaller production spaces. Rather than print mass numbers of parts held in inventory, manufacturers will print on demand and customize without additional cost.

As such, 3D printing has the potential to disrupt traditional supply chains and distribution channels. With 3D printing, manufacturing today is digitally enabled, distributed, and democratized. In time, it will probably become easier to use, affordable, and available to anyone with access to the Internet.

Despite the significant promise of 3D printing, the technology still faces several constraints to universal adoption. At the lower end of the market, some industry experts argue that the range of materials used in producing household products and requisite skills makes the technology impractical for consumers.[8]

At the higher end of the market, 3D printers suitable for advanced industrial processes continue to require high capital investments. Companies may resist adopting the new technology if they have significant sunk costs in machinery for traditional manufacturing processes. The speed and resolution of 3D printers are improving each year but have some distance to go to meet industry expectations for mass production. The prices of materials, due to a limited number of suppliers charging proprietary prices, remain high relative to those for traditional manufacturing. Given its status as a new field, standards need to be developed to certify the quality and performance of parts produced by 3D printers. Moreover, engineers schooled on traditional methods need to be retrained as the number of experienced operators is lagging behind demand for the technology.

That said, the capabilities, versatility, and user-friendliness of 3D printers are improving at a rapid pace, reducing existing limitations of the technology for broader use. In the future, sensors and monitors integrated into 3D printers will send alerts in the event of mistakes/failures, eventually allowing users to "just press print" for advanced metal components.

The Risks

Despite the many benefits, additive manufacturing has significant implications for national security and is likely to generate some new risks for the WMD space. In theory, 3D printing will allow state and nonstate actors to circumvent the need for engineers and scientists with tacit knowledge.[9] Digital blueprints, designed and tested by scientists and engineers, would embed a certain level of technical expertise in electronic form. This "embedded expertise" would allow people without traditional manufacturing skills to produce parts or objects by simply loading up a 3D printer with the required raw materials and then pressing the print button. Of course, these blueprints do not include post-print finishing or assembly, but a digital build file could come with instructions for finishing and assembly.

Several years ago, 3D printing became known as a potential enabler of mischief. In 2012, Cody Wilson, a second-year law student at the University of Texas, and his friends, naming themselves "Defense Distributed," launched the "Wiki Weapon Project" to develop a 3D-printed plastic gun using a low-cost, open-source 3D printer known as a RepRap. [10] The group successfully produced the "Liberator," which was capable of firing a .22 caliber bullet, and released the blueprint online. The design was downloaded 100,000 times in just 2 days before the U.S. State Department stepped in, demanding the removal of the blueprint file from the Web site under the International Traffic in Arms Regulations. Nonetheless, the file remains available on disreputable file-sharing Web sites.

In the near term, 3D printing may enhance the capabilities of state and nonstate actors in similar ways with national security implications, from enabling the printing of counterfeit goods to the development of advanced conventional weapons and even non-nuclear components for nuclear weapons.

Additive manufacturing enables the production of counterfeit goods. "With a high-resolution laser scanner and a good enough [additive manufacturing] system, a product counterfeiter could potentially replicate all sorts of luxury items."[11] Using the same principles, state actors may someday be able to reverse-engineer components, for example, of a uranium enrichment program and circumvent steps in the development process.

With the ability to easily embed objects within objects, additive manufacturing can enhance concealment and complicate detection by authorities. Using 3D printers, nonstate actors could print seamless Trojan horses—objects that appear normal but contain illicit substances such as drugs or explosives that are embedded into the object itself. 3D-printed and embedded electronics could be used for RFID chips, cameras, or other tracking devices. These strategies will complicate detection by authorities with existing techniques (for example, x-rays).

Converging with information technology, additive manufacturing introduces new cybersecurity challenges. The inherently digital character of 3D printers means that many machines will become part of the growing "Internet of things," leading to questions about their security from cyberattacks. Additionally, the security of the CAD software used to design digital models must also be scrutinized for vulnerabilities to ensure that finished products are printed to the intended design. Loopholes in the software could allow actors to engage in sophisticated sabotage actions against advanced militaries.

Leading manufacturers and advanced militaries are exploring the potential of 3D printing to produce advanced weapons systems. Raytheon recently announced the capability to print over 80 percent of a guided missile's components, with 100 percent capability a stated near-term goal.[12] This would allow soldiers to 3D-print guided missiles in the field as needed. These sensitive "build files" need to be secured against hacking by both states and nonstate actors. If state and nonstate actors were able to gain access to sensitive digital files, they may be able to gain access to technology traditionally only available to advanced militaries.

Additive manufacturing may lower barriers to nuclear weapons acquisition and reduce program signatures. Given its small footprint, the use of 3D printing for manufacturing non-nuclear components of nuclear weapons would lead to significant reduction in required factory floor space. Moreover, additive manufacturing machine operators do not need to know what they are making and would not likely recognize nuclear components. The manufacturing process could be distributed over several plants to further conceal the intended purpose.

Metal additive manufacturing offers a powerful technology for producing non-nuclear components. Many metals used for making non-nuclear components such as maraging steel existed before the emergence of 3D printing. If a state cannot acquire maraging steel powder, atomizers are readily available and inexpensive. Although uranium is a metal and exists in powder form, the technology is not practically suitable for printing pits with special nuclear material because the powder bed for the laser sintering printers would have to contain multiple critical masses.

Current efforts under way to support the U.S. nuclear weapons program demonstrate the massive advantages offered by the technology for producing non-nuclear components. The Kansas City plant, part of the U.S. nuclear weapons complex, has been using 3D printing to design and produce non-nuclear components to improve the way they are designed and manufactured.[13] Kansas City plant engineers experimented with lower-end 3D printers to see what they could do with the technology—they found advantages in quick and easy production value at these lower-end desktop printers and saved $10 million in development costs using 30 MakerBot printers for prototyping.[14]

However, the advantages of additive manufacturing for current nuclear weapons states are not guaranteed. Advanced nuclear states may already have millions of dollars of sunk costs in their nuclear program, and the existing technology is still meeting their needs. New proliferators, on the other hand, might seek to exploit the benefits of 3D printing if their scientists already have training on the technology. This would allow them to speed up the development timeline. If a state were simply able to download and print plans for advanced centrifuges or parts, this would circumvent the decades of development undertaken by existing nuclear weapons states.[15]

Over the longer term, the cutting edge of additive manufacturing will add several new risk dimensions, including hybrid technologies, bioprinting, and microreactor printing.

Multi-material printing and hybrid technologies—combining 3D printing, finishing, and assembly—may enable states and nonstate actors to someday print a robot that walks off the printer on its own, with no assembly required. Such capabilities would allow for the manufacturing of functional systems without the tacit knowledge that is usually required.

3D printing may also enable the development of chemical weapons. Additive manufacturing is being used to make miniaturized fluidic reaction ware devices that can produce chemical syntheses in just a few hours. This may enable state and nonstate actors to more easily develop chemical agents in the future.[16]

In the United Kingdom, Dr. Leroy Cronin of the University of Glasgow wants to create downloadable chemistry, with the ultimate aim of allowing people to "print" their own pharmaceuticals at home. In his lab, his team has used a 3D printer costing less than $2,000 to build a prototype chemical 3D printer, which could be programmed to make basic chemical reactions and produce different molecules. After the microreactors are printed, he injects "chemical inks" to create sequenced reactions. He envisions that it should someday be possible with a relatively small number of inks to make any organic molecule.[17]

The Opportunities

Given its many benefits for the manufacturing industry, 3D printing may offer new opportunities and solutions to defense communities for countering WMD, including on demand, production, customization, printing in the field, and new materials.

Additive manufacturing allows for the production of small numbers of items quickly and cheaply—and then a reworked version with no additional cost for the design modifications. This is particularly advantageous when there is no need for economy of scale. Whereas new prototype designs usually required making new molds or dies in the past, 3D printing enables the production of parts individually and on demand, significantly reducing the overall cost of prototypes and customization. These features allow for rapid prototyping, for example, of WMD detection technology, urgent military or medical countermeasures, and/or custom-printed masks to protect against chemical and biological agents.

Since the 3D printer can be housed in a much smaller space compared to the traditional manufacturing line, parts can be manufactured in the field, simplifying logistics. To support chemical, biological, radiological, and nuclear (CBRN) operations, one could simply send 3D printers and raw materials into the field and transmit designs electronically. The U.S. Navy is experimenting with 3-D printers aboard ships that allow them to print drones custom tailored to mission objectives from a base set of supplies.[18] The Navy is also looking at 3D printing to find cost savings for its logistical supply chains. Submarines are typically at sea for 4 to 6 months and need to carry a full load of supplies. With a more compact supply of powders and raw materials, submarine crew could simply produce needed parts on board.

As 3D printing converges with new materials such as biological tissues, carbon fiber, and nanomaterials, the technology could offer new solutions for countering WMD in the future. Bioprinting currently enables the printing of cells and organ systems for the purpose of drug testing and the development of new medical countermeasures.

Meanwhile, carbon fiber printing produces lighter, stronger parts than other manufacturing materials.[19] Printing with composite nanomaterials offers increased strength (tensile, fracture, yield stresses), improved thermal stability, reduced or increased density, decreased shrinkage, and enhanced electrical conductivity.[20] Important challenges remain, however, to the use of nanomaterials in additive manufacturing including material accumulations in the machine, rough surface finishes, increased part porosity, nozzle clogging, low resolution, and difficulty retaining part shape.

Conclusion

The impact of additive manufacturing as an enabler of WMD remains mostly in the theoretical realm at the current time. States and nonstate actors have not yet harnessed the technology to develop new WMD. Even so, the United States has already begun to leverage the benefits of additive manufacturing to print non-nuclear components to support its nuclear arsenal. Additionally, the U.S. defense community has started to explore the value of using 3D printing to enhance capabilities to counter WMD. As the technology advances and becomes cheaper and easier to use, it will offer states and nonstate actors a powerful enabling tool in the area of WMD.

---

[7] Andrew Zaleski, "Here's Why 2016 Could be 3D Printing's Breakout Year," *Fortune,* 30 December 2015, <http://fortune.com/2015/12/30/2016-consumer-3d-printing/>.

[8] Connor M. McNulty, Neyla Arnas, and Thomas A. Campbell, "Toward the Printed World: Additive Manufacturing and Implications for National Security," *Defense Horizons* 37 (September 2012), <http://www.dtic.mil/dtic/tr/fulltext/u2/a577162.pdf>.

[9] Natasha Bajema, "3D Printing: Enabler of Mass Destruction?" *Nuclear Spin Cycle Blog*, 28 April 2016, <https://natashabajema.com/2016/04/28/3d-printing-enabler-of-mass-destruction/>.

[10] 3D printers using the material extrusion process and thermoplastic as the raw material are widely available on the commercial market for several hundred dollars. Adam Popescu, "Cody Wilson: The Man Who Wants Americans to Print Their Own 3D Guns," *The Guardian,* 6 June 2016, <https://www.theguardian.com/us-news/2016/jun/06/cody-wilson-3d-guns-printing-firearms-lower-receivers>.

[11] Thomas A. Campbell and William J. Cass, "3-D Printing Will Be a Counterfeiter's Best Friend—Why We Need to Rethink Intellectual Property for the Era of Additive Manufacturing," *Scientific American*, 5 December 2013, <http://www.scientificamerican.com/article.cfm?id=3-d-printing-will-be-a-counterfeiters-best-friend>.

[12] Raytheon, "To Print a Missile: Raytheon Research Points to 3-D Printing for Tomorrow's Technology," 19 March 2016, <http://www.raytheon.com/news/feature/3d_printing.html>.

[13] See Tyler Koslow, "Keeping Nuclear Weapons Secure with 3D Printing at the National Security Campus," *3D Printing Industry,* 28 October 2015, <http://3dprintingindustry.com/news/keeping-nuclear-weapons-secure-with-3d-printing-60927/>.

[14] Ibid.

[15] For a discussion on how 3D printing could enable the development of nuclear weapons, see Matthew Kroenig and Tristan Volpe, "3D Printing the Bomb? The Nuclear Nonproliferation Challenge," *The Washington Quarterly* (Fall 2015): 7–19, <https://twq.elliott.gwu.edu/sites/twq.elliott.gwu.edu/files/downloads/TWQ_Fall2015_Kroenig-Volpe.pdf>.

[16] W. Baltzley, "3D-printed Micro Reactors," *Chemistry World* (blog), 1 March 2013, <https://digitalmatternet.wordpress.com/2013/0

3/01/3d-printed-micro-reactors-chemistry-world/>.

[17] See Lee Cronin, "Print Your Own Medicine," *Ted Talk,* June 2012, <https://www.ted.com/talks/lee_cronin_print_your_own_medicine?language=en>.

[18] Eddie Krassenstein, "US Navy is 3D Printing Custom Drones Onboard the USS Essex," *3DPrint.com,* 30 June 2015, <https://3dprint.com/85654/us-navy-3d-printed-drones/>.

[19] Kira, "The Strongest Players in Carbon Fiber 3d printing today," *3ders.org*, 29 February 2016, <http://www.3ders.org/articles/20160229-the-strongest-players-in-carbon-fiber-3d-printing-today.html>.

[20] Olga S. Ivanova, Christopher B. Williams, and Thomas A. Campbell, "Additive Manufacturing (AM) and Nanotechnology: Promises and Challenges," *Rapid Prototyping Journal* 19, Issue 5 (2013): 353–364, doi: 10.1108/RPJ-12-2011-0127.

Advanced Robotics

Advanced robotics generates both new risks and opportunities for the WMD space. Increasingly, sophisticated robots are available commercially for industrial and domestic use, with commercial drones at the forefront of this trend. Whereas commercial drones offer states and nonstate actors a potential delivery system for WMD, the wide range of robotics across the sea, land, and air domains enhances defense capabilities for countering WMD by providing agile and cheap platforms for detecting WMD and operating in a hazardous environment.

Technology Overview

The development of advanced robotics, a branch of mechanical engineering, electrical engineering, and computer science, began in the 1960s with a basic robotic arm designed to perform tasks that were difficult or too dangerous for humans. The field of advanced robotics has tracked closely with advances in computing, artificial intelligence (AI), and energy storage. Today, increasingly sophisticated robots are widely available on the commercial market and prices are dropping dramatically, expanding their use.[21]

A robot is a reprogrammable, multifunctional manipulator designed to move material, parts, tools, or specialized devices through various programmed functions for the performance of a variety of tasks.[22] All robots have certain defining features including a mechanical structure designed to carry out a specific task, electrical components that power and control the machinery, and some level of computer programming code.

Artificial intelligence refers to near-human, human, or super-human ability to respond to a complex environment. Robots are intelligent systems that apply a certain level of AI to a specific problem or domain. The sophistication of the computer program embedded in a robot determines its level of autonomy and the nature of its human oversight.

Weak artificial intelligence, the cognitive ability to solve specific problems or perform certain tasks, has supported a broad range of applications for many decades.[23] Robots using weak AI are controlled by humans. A remote-control robot has programming with a preexisting set of commands that it will perform when it receives a signal from a control source, typically a human with a remote control. This is referred to as "in the loop," in which a human confirms actions, denies actions outside designed constraints, and denies actions outside the operational context.

On the opposite side of the spectrum are autonomous robots, which are intelligent machines capable of performing tasks in the world by themselves normally requiring human intelligence (e.g., perception, conversation, decision-making), without explicit human control.[24] This is referred to as "out of the loop," since machines function without the ability of humans to intervene.

To be autonomous, a system must have the capability to independently compose and select among different courses of action to accomplish goals based on its knowledge and understanding of the world, itself, and the situation.[25] In the future, robots will be increasingly able to operate autonomously, without human intervention.[26]

Hybrid systems involve both elements of human control and autonomy. This is referred to as "on the loop," in which a human can allow actions outside designed constraints or outside operational context in order to take advantage of evolving context.

In addition to different levels of complexity, robots can be developed to address many types of problems or for use in and across many different domains, including industry, commerce, land, sea, and air. Of these domains, UAVs in particular (or "drones" as they are popularly known) are taking off in the civilian and commercial sectors.[27]

Industry experts are hailing the year 2016 as the dawn of the drone age. Consumer sales are expected to reach four million in 2016 and 16 million by 2020.[28] The number of operators of drones, both large and small, is rising rapidly. Many affordable commercial drones offer significant off-the-shelf capabilities. UAV technology has enabled thousands of individuals the opportunity to enter the field of aviation, with comparably little training and oversight.

In addition to the growing market for civilian drones, the commercial drone sector is booming. Companies like Amazon and Google, among others, are developing drones as a platform for making rapid deliveries across cities. According to the Federal Aviation Administration, the most significant uses of UAVs come from agriculture, photography, and mapping.

In the agricultural sector, for example, drones allow for precision farming. This method reduces the amount of chemicals sprayed on crops by precisely dusting crops. Drones can also fly close to the ground and stream videos to provide a comprehensive picture of the farm, allowing producers to be more efficient in addressing growth issues and even monitoring unexpected pests. This can help farmers address levels of water damage or dryness and aid in the monitoring of large crops that need a lot of attention.

Although robotics are becoming more accessible, cheaper systems remain limited in terms of autonomy and capabilities. The utility of drones for many applications is constrained by range, flight time, and payload or carry weight (enabled by battery/energy storage). Typically, there are trade-offs between flight time and carry weight. The heavier the carry weight, the shorter the flight time. Much of the promise of robotics remains a prospect of the future. Engineers have thus far not been able to build a machine capable of human-like cognition. However, advances in computing and energy storage may offer near-term leaps forward in the field of advanced robotics.

The Risks

Among the wide range of robotics coming of age in the neart erm, policymakers are most immediately concerned about the use of hobbyist and commercial drones for potential mischief by nonstate actors and the development of advanced UAVs by state actors as an asymmetrical capability vis-à-vis high-tech platforms such as fighter jets.[29]

Enabling aerial operations, drones can provide unfettered access to targets in ways that terrorists could previously only dream about and security planners have not had to worry about. Airborne improvised explosive devices (IEDs) could be used to attack people, infrastructure, or aircraft, among many other possible targets, where large destructive power may not be necessary to cause tremendous amounts of damage. Hobbyist drones have limited payloads and ranges but can still be used for disproportionate effects.

For example, in September 2013 in Germany, a political protester flew a drone within feet of German Chancellor Angela Merkel and Defense Minister Thomas de Maiziere, before it crash-landed next to them.[30] Armed with even a small amount of explosive, fragments or shrapnel could have killed or maimed two members of Germany's leadership.

In early November 2014, multiple drones were sighted over French nuclear power plants, in what was described as a "provocation of French authorities."[31] A squadron of drones armed with explosives and detonated in certain positions may be able to cause significant damage to expensive infrastructure.

Military aircraft and other high-technology platforms are not immune to this threat. A small number of expendable drones could cause significant damage to a military aircraft costing hundreds of millions of dollars.[32] The number of drones is scalable, whereas explosive capacity is limited by the physical capability of each individual drone.

In 2009, US Airways Flight 1549 had to make an emergency landing on the Hudson River after colliding with a gaggle of Canada geese.[33] Compared to a bird, a drone consisting of metal, hard plastics, batteries, and electronics could do far more damage and has the potential to take down a passenger jet.

As advances in artificial intelligence are mated with drone technology, drones will begin to perform previously pilot-controlled tasks (navigation, coordination, targeting) autonomously, without the need for input from the primary operator. Multiple drones possessing these autonomous capabilities could "swarm" a target and offer a powerful asymmetric capability to both states and nonstate actors.

Carrying biological, chemical, or radiological materials, drones offer an extremely agile delivery platform for WMD, even if they are still limited to a small payload. On 24 April 2015, a Japanese man landed a drone containing radioactive material on the roof of Japanese Prime Minister Shinzo Abe's office in protest of Japan's nuclear energy policy. In October 2016, ISIS used a drone loaded with explosives for the first time in an attack that killed two soldiers and injured two others.[34] Given the use of chlorine and mustard agents by ISIS, it is conceivable that insurgents might use drones as delivery vehicles for chemical and biological agents in the near future.

Drones flown over crowded venues or around aircraft at airports do not have to be lethally armed to lead to panicked responses from people, companies, and authorities and therefore could be used to instill fear into a target.

Converging with 3D printing, some drones can now be printed relatively quickly; they are lighter, travel farther, and have greater capacity to carry payloads than other remote-controlled electronics. For example, researchers at the University of Virginia were tasked to create a drone that was similar to current military drones but that could be 3D-printed and that utilized only off-the-shelf parts. The Razor drone is tailorable to meet operational needs and is capable of variable flight time (45+ minutes) and speeds (40+ mph). Its cost was about $2,500, most of which was for the cellphone that acts as the entire electronics package of the drone and is capable of command and control via cell signal.[35] The Razor drone can be built in just over 24 hours.

The costs are expected to drop even further. In March 2014, engineers in the United Kingdom successfully developed a 3D-printed drone that cost $9 per copy and could be built and assembled in less than 24 hours.[36] If a nonstate actor group acquired the blueprint and 10 printers, it could print 10 per day and 300 per month at a cost of $2,700 plus the cost of the printers.[37]

The Opportunities

Advanced robotics offer ideal platforms to perform dangerous counter-WMD missions including surveillance and detection, decontamination, and operations.

Cheap, expendable, and often tiny in size, robotics offers a powerful tool for surveillance and detection missions. The U.S. Army is developing the Micro Autonomous Systems and Technology (MAST). These tiny insect-shaped ground and aerial robots are designed to assist soldiers with rapid and mobile intelligence, surveillance, and reconnaissance missions in high-risk zones.[38] Microbots can capitalize on their size to move quietly and easily access small spaces. If a unit approaches a building and needs to know what is inside, for example, the soldiers could deploy a reconnaissance team of microbots. The robots could penetrate the building undetected, search the interior, map the layout, and provide data on the building's occupants and their locations.

The U.S. Army also developed the WMD Aerial Collection System, an unmanned capability designed to assess the presence of airborne CBRN material during military operations. The UAV mounted with trackers and collectors is capable of locating, intercepting, and collecting aerial samples from a CBRN plume for analysis in a laboratory facility. The system allows for in-flight detection reporting.

Enhanced by AI and 3D printing technologies, small teams of MAST robots are being designed to be autonomous and capable of coordination or "swarming."[39] These robots are envisioned to support soldiers with improved tactical situational awareness in urban and complex terrain. In the future, the U.S. Army hopes to be able to 3D-print drones while on mission in less than 24 hours.[40]

Robotics are ideal platforms for detecting the presence of CBRN materials in hostile areas. The U.S. Army partnered with Carnegie Mellon University and Sikorsky Aircraft to design an autonomous ground vehicle delivered by UAV (modified Black Hawk helicopter) into hostile or inaccessible areas equipped with chemical, biological, and radiological sensors for missions in contaminated areas.[41]

Robots can safely operate in hazardous environments and assist in counter-WMD missions including decontamination and operations. The U.S. Army is working to develop a robot capable of locating, lifting, and carrying wounded soldiers out of dangerous zones to safety for treatment. The Battlefield Extraction-Assist Robot (BEAR) is currently designed to be remote-controlled by combat medics, but developers are working to expand its capacity to assume semi-autonomous tasks. The BEAR has a "teddy bear" face to reassure injured soldiers and can be used for other missions such as search and rescue, handling hazardous materials, surveillance and reconnaissance, mine inspection, lifting hospital patients, or even warehouse automation.[42]

Leveraging robots' ability to operate in hazardous environments, the Department of Defense contracted with Boston Dynamics and the Midwest Research Institute to create a robot capable of testing chemical warfare suits called the PETMAN.[43] Once completed, the PETMAN weighed 180 pounds and was capable of running 4.4 mph on smooth surfaces. Tests conducted with these robots ensure that the suits maintain their integrity in a contaminated environment while moving in the same way a human would.

The U.S. Navy has developed the Battlespace Preparation Autonomous Underwater Vehicle (BPAUV), a small, fast, autonomous underwater robot, primarily to handle its mine countermeasure mission in shallow water.[44] With its compact size and accurate navigation, the BPAUV can be operated from a ship or boat, function in a variety of weather conditions, and collect high-quality imagery necessary for successful operations. Other applications include unexploded ordnance, anti-submarine warfare, and oceanography.

Conclusion

Robotics offer powerful, and often cheap, platforms for performing a wide range of tasks. For nonstate actors, drones may serve as a readily available delivery platform for an IED or WMD. For advanced states and militaries, robotics offer significant advantages for operating in hazardous environments on land, in the sea, and in the air.

---

[21] James Kadtke and Linton Wells, *Policy Challenges of Accelerating Technological Change: Security Policy and Strategy Implications of Parallel Scientific Revolutions* (Washington, DC: NDU Press, 2014), 43, <http://ctnsp.dodlive.mil/files/2014/09/DTP106.pdf>.

[22] As defined by the Robot Institute of America in 1979.

[23] As defined by Kadte and Wells in *Policy Challenges of Accelerating Technological Change*.

[24] As defined by George Bekey in *Autonomous Robots: From Biological Inspiration to Implementation and Control* (Cambridge, MA: The MIT Press, 2005).

[25] L.G. Shattuck, "Transitioning to Autonomy: A Humans Systems Integration Perspective," paper presented at the Autonomy Workshop, NASA Ames Conference Center, Moffett Field, CA, 10–12 March 2015, <https://human-factors.arc.nasa.gov/workshop/autonomy/download/presentations/Shaddock%20.pdf>.

[26] As defined by Kadte and Wells.

[27] Unmanned aerial vehicles (UAVs) are defined by the Department of Defense as powered aerial vehicles that do not carry a human operator, use aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 12

April 2001, <http://jitc.fhu.disa.mil/jitc_dri/pdfs/jp1_02.pdf>.

[28] Adario Strange, "2016 Will Be the Dawn of the Drone Age," *Mashable,* 21 December 2015, <http://mashable.com/2015/12/21/the-year-in-drones/#VVGsAqeAr5qN>.

[29] For an in-depth assessment of the nonstate actor threat, see Don Rassler, *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology* (Westpoint, NY: Combating Terrorism Center, 2016), <https://www.ctc.usma.edu/v2/wp-content/uploads/2016/10/Drones-Report.pdf>.

[30] Friederike Heine, "German Election: Merkel Buzzed by Mini-Drone at Campaign Event," *Spiegel Online, 16* September 2013, <http://www.spiegel.de/international/germany/merkel-campaign-event-visited-by-mini-drone-a-922495.html>.

[31] John Lichfield, "French Government on High Alert After Unexplained Drone Flights over Nuclear Power Stations," *Independent,* 9 November 2014, <http://www.independent.co.uk/news/world/europe/french-government-on-high-alert-after-unexplained-drone-flights-over-nuclear-power-stations-9850138.html>.

[32] T. X. Hammes, "Cheap Technology Will Challenge U.S. Tactical Dominance," *Joint Force Quarterly* 81 (2nd Quarter 2016), 76–85, <http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-81/jfq-81_76-85_Hammes.pdf>.

[33] NTIS Number: PB2010-910403 "Loss of Thrust in Both Engines, US Airways Flight 1549 Airbus Industry A320-214, N106US," *National Transportation Safety Board,* 15 January 2009, <http://www.ntsb.gov/investigations/accidentreports/pages/AAR1003.aspx>.

[34] Jamie Crawford, "Report Warns of ISIS Developing Drones for Chemical Attacks," *CNN Politics*, 20 October 2016, <http://www.cnn.com/2016/10/20/politics/terrorist-groups-and-drones/>.

[35] Jordan Golson, "A Military-Grade Drone that Can Be Printed Anywhere," *Wired*, 16 September 2014, <https://www.wired.com/2014/09/military-grade-drone-can-printed-anywhere/>.

[36] Victoria Woollaston, "Cheap Drones Are Coming! Researchers Successfully Build and Fly a Low-cost 3D Printed Disposable Aircraft," *Daily Mail Science,* 28 March 2014, <http://www.dailymail.co.uk/sciencetech/article-2591533/Cheap-3D-printed-drones-coming-Researchers-successfully-build-fly-low-cost-DISPOSABLE-aircraft.html>.

[37] T.X. Hammes, "Technologies Converge and Power Diffuses: The Evolution of Small, Smart and Cheap Weapons," *Policy Analysis,* no. 786 (January 2016): 1–14, <https://object.cato.org/sites/cato.org/files/pubs/pdf/pa786-updated.pdf>.

[38] Tracie Dean, "Micro Autonomous Systems and Technology Collaborative Technology Alliance: Researchers Aggressively Explore Miniature Robots to Enhance Capabilities," U.S. Army Research Laboratory, 13 June 2014, <http://www.arl.army.mil/www/default.cfm/default.cfm?article=2485>.

[39] Joshua Topolsky, "Bug-Bot Video Reveals Swarming Drones, Extreme Rocking," *Engadget,* 4 May 2008, <http://www.engadget.com/2008/05/04/bug-bot-video-reveals-swarming-drones-extreme-rocking/>.

[40] Kelsey Atherton, "Army Wants Drones on Demand, 3D-Printed in 24 Hours or Less: A Drone Today for a Battle Tomorrow," *Popular Science,* 19 February 2016, <http://www.popsci.com/army-wants-to-3d-print-drones-in-24-hours>.

[41] AMRDEC Public Affairs, "Army, Industry, Academia Partner to Demonstrate New Technologies," *Army Technology,* 9 November 2015, <http://armytechnology.armylive.dodlive.mil/index.php/2015/11/20/army-industry-academia-parter-to-demonstrate-new-technologies/>;

Matt Brown, "Extending the Reach of the Warfighter through Robotics (ERWR): CBRN Demonstration Project," <http://www.ecbc.army.mil/about/posters/2015/D22.pdf>.

[42] Darren Quick, "Battlefield Extraction-Assist Robot to Ferry Wounded to Safety," *New Atlas, 25* November 2010, <http://www.gizmag.com/battlefield-extraction-assist-robot/17059/>.

[43] Defense Threat Reduction Agency, "WMD Aerial Collection System (WACS)," <http://globalsecurity.cubic.com/?q=system/files/infographics/WACS%20Info%20Sheet.pdf>.

[44] Bluefin Robotics, "Bluefin-21 BPAUV," 3 December 2010, <http://www.bluefinrobotics.com/assets/Sell-Sheets/Bluefin-21-BPAUV-Product-Sheet.pdf>.

Nanotechnology

Nanotechnology produces new risks and opportunities for the WMD space. Mostly considered a materials science to date, nanotechnology functions as an enabling technology by making other technologies work better or do things not previously possible.

Technology Overview

Nanoscience emerged as a field in 1981 with the development of microscopes capable of seeing individual atoms and operating at the nanoscale (1 to 100 nanometers). The prefix "nano" means one-billionth or 10^{-9}; one nanometer is one-billionth of a meter. Nanotechnology—that is, applied science and engineering—involves manipulation and control of atoms and molecules to leverage the unique properties of materials at the nanoscale.

At a normal scale, common materials have a range of different physical, chemical, mechanical, and optical properties. However, matter behaves quite differently at the nanoscale, deviating from the laws of physics that apply to bigger objects and operating according to a new set of rules (quantum effects) that alter the electrical, optical, thermal, and mechanical properties of materials.

When the particle size of a material is reduced to the nanoscale, it can have different melting points, fluorescence, electrical conductivity, magnetic permeability, and chemical reactivity. For example, copper (normally opaque) is transparent at the nanoscale, aluminum (normally stable) becomes combustible, and gold (normally a solid and gold-colored) becomes a liquid and a reddish/purplish color.

Additionally, properties at the nanoscale are "tunable," meaning that scientists can adjust the material properties by changing the size of the particle (for example, dial up or dial down fluorescence of a material). Another unique feature of nanomaterials is surface area. For the same mass of materials, nanoscale materials have a relatively larger surface area. Larger surface area in nanomaterials has advantages in different applications.

Different types of nanomaterials are named for their shapes and dimensions; they are tubes, wires, particles, films, flakes, or shells that have one or more nanometer-sized dimension. For example, carbon nanotubes have a diameter in the nanoscale, but their length can be several hundred nanometers or longer. Similarly, nanofilms have a thickness in nanoscale, but their other dimensions are larger.

Manufacturing using carbon nanomaterials is leading to improvements among existing products. Carbon nanotubes are light, stiff, and strong fibers that have outstanding mechanical and electronic properties and are good thermal conductors. In addition, the tensile strength of carbon nanotubes is six to seven times that of steel. If used in place of steel and other metals, they enable products to become lighter and stronger.

Graphene is a flat one-atom-thick sheet of carbon and exhibits thermal stability and electrical conductivity. It is also one of the lightest material ever discovered, weighing seven times less than an equal volume of air.[45] The minimal weight of graphene combined with its conductivity makes the material a powerful alternative to conventional materials used to produce electronics.

Advanced Functional Fabrics of America is producing carbon fibers and yarns that have ten times the strength of steel.[46] A typical commercial aircraft has about 8,000 pounds of wires on board.[47] Instead of conventional copper wire, composites containing carbon at the nanoscale can be used to produce the wiring needed for aircraft and commercial drones, reducing the weight and using less energy to fly.[48] In addition to reduced fuel consumption, wiring made from carbon nanotubes conducts electricity with improved efficiency.[49]

Nanomanufacturing involves two distinct approaches to producing nanomaterials. Top-down processes reduce materials down to the nanoscale. By taking the material around us, reducing it to the nanoscale, and rearranging atoms, nanotechnology offers new capabilities to engineer materials with new and precisely tuned properties, which will enhance many existing products.

The bottom-up approach makes products by building them up from atoms and molecules. In this sense, nanotechnology replicates what already is possible in the field of synthetic biology.

Manufacturing at the nanoscale leverages unique new properties to make products stronger, more durable, lightweight, anti-reflective, conductive, and even water-resistant. Consumer products made with nanomaterials first began to appear on the marketplace in the early 2000s. Today, companies around the world manufacture nanomaterials to make new products and improve existing ones. More than 800 everyday commercial products use nanoscale materials and processes.[50]

According to research by Lux Research (supported by the National Science Foundation), nanotechnology has become a global enterprise. In 2014, governments and the private sector worldwide invested over $18.1 billion in nanotechnology (33 percent of that amount in the United States). Within the United States, corporate spending on research and development reached $4 billion, significantly exceeding the $1.67 billion invested by the U.S. Government. The global value of nano-enabled products is expected to reach $3.6 trillion by 2018.[51]

Convergence with other emerging technologies is expected to make nanotechnology even more potent as an enabling technology. For example, advances in nanotechnology will enable the next generation of AI and allow for more sophisticated robotics and computing power. New nanomaterials will allow for higher resolutions in 3D printing. In the distant future, molecules, delivered by nanoparticles into the human body, may be capable of gene editing to treat disease.

Despite all its promise, nanotechnology has several limitations that will constraint its impact more broadly in the near term. Nanotechnology requires specialized and expensive equipment, which could serve as a barrier to less advanced actors. In addition, the need for extensive training and significant tacit knowledge makes the technology inaccessible and economically costly for many actors.

The Risks

Nanotechnology will produce several new risks for the WMD space in the future for the delivery of WMD and development of high explosives. As the technology advances and new discoveries are made, this list is likely to increase. However, as noted above, there are still significant barriers to using nanotechnology. Economic cost, sophisticated equipment, and a high level of training and tacit knowledge will prevent less advanced state actors and nonstate actors from exploiting the advantages of nanotechnology in the near term.

Nanotechnology may enhance the delivery of WMD by enabling lighter, more capable drones. Fears about the potential use of commercial drones by nonstate actor for mischief are on the rise. Today, off-the-shelf commercial drones remain constrained in terms of their range, flight time, and payload, all of which are affected by the weight of the drone and battery capacity. Nanomaterials are expected to reduce these constraints and expand the capabilities of commercial drones.

Materials science at the nanoscale is producing more powerful materials with higher strength-to-weight ratios than steel and better electrical conductivity. As new nanomaterials are used in the manufacturing of drones and batteries, commercial drones will have longer flight times and longer ranges and be capable of carrying heavier payloads.

Nanotechnology may also someday facilitate targeted delivery of biological and chemical agents. Fullerenes are spherical carbon-cage molecules with 60 or more carbon atoms that exhibit properties making the material suitable for medical use, specifically the delivery of targeted medicine. In addition to their small size, customized surface, and solubility, fullerenes are strong antioxidants and capable of binding with antibiotics to target resistant bacteria or other treatments for targeting cancer cells. The fullerene is used to transport the drug into diseased cells.[52] These nanomaterials could also be used as Trojan horses for delivering biological and chemical agents.

Exploiting new developments in the delivery of drugs, nanotechnology might also be used to improve dispersal of agents for a more targeted delivery.[53] Given their size, nanomaterials are capable of crossing the blood-brain barrier, allowing rare access to the brain. If effectively dispersed, a small number of nanoparticles containing a chemical or biological agent (assuming the materials being delivered by the nanoparticles are successfully reduced to the nanoscale) could conceivably traverse the olfactory nerve in the nose (a backdoor route to the brain).

Nanotechnology may have indirect enabling effects for the WMD space in the area of nanoenergetics and high explosives. If nanoexplosives are combined with other emerging technologies (for example, commercial drones and swarming), the technology could contribute to the development of weapons with mass effects by state and nonstate actors.[54]

The field of nanoenergetics takes advantage of the large surface area of nanomaterials to increase the rate of reaction in explosive materials and produce a more powerful explosion. The use of nanomaterials in explosives allows for more precise control of fuel combustion and detonation, making possible smaller, more powerful rockets, propellants, bombs, and explosive devices. This means that smaller platforms, like commercial drones, will be able to carry greater destructive power and pose a threat to harder, more sophisticated targets.[55]

The Opportunities

In the near term, nanotechnology holds tremendous promise for producing new solutions to counter threats posed by WMD, including the development of new medical countermeasures, advances in sensing, and improved ability for response to WMD incidents.

Nanotechnology is contributing to advances in medicine and medical countermeasures for people exposed to WMD materials. Nanoscale materials are found in nature. Moreover, chemistry and biology often operate at the nanoscale. For example, hemoglobin, the oxygen-transporting protein found in red blood cells, is 5.5 nanometers in diameter.

Nanomaterials such as quantum dots and fullerenes are about the same size as biological materials such as liposomes or dendrimers. Quantum dots are man-made crystals capable of semi-conduction. By varying the diameter/size of the quantum dot, scientists and engineers can change the wavelength of light that it emits. This feature is exploited for high-definition LED television sets, but also for illuminating tumors in the body during surgical procedures.

Nanomaterials are powerful because they can be put in the bloodstream to combat disease and are small enough to cross biological barriers such as the blood-brain barrier. As such, they can be used to target cancer cells or deliver drugs to specific areas within the body. However, at the current phase of development, crossing two barriers remains challenging even for nanoparticles. For the WMD space, nanoparticles may be able to deliver antidotes to viruses or chemical agents, allowing for the development of new and more effective medical countermeasures.

Nanomaterials exhibit powerful capabilities for sensing, given their large ratio of surface area to mass. Sensors using nanomaterials have better selectivity, better specificity, lower power demands, and lower volume than conventional sensors. These sensors are able to discriminate between hazardous and nonhazardous substances and more exactly determine the identity of a detected substance. Nanomaterials also improve the speed, accuracy, and sensitivity of assays designed to detect protein toxins from complex samples.

Given the range of properties of nanomaterials, nanoparticles can act as sensors, antennas, and communication systems. Smaller, more powerful sensors will enable rapid detection, identification, and quantification of biological and chemical agents in the field. Moreover, nanomaterials will enable the development of flexible armor with medical sensors, medical treatment, and integrated chemical and biological sensing systems woven into fabric.[56]

Finally, nanotechnology will enhance emergency response capabilities in the event of a WMD incident. In addition to WMD detection, nanomaterials can be used to develop lightweight communication devices for first responders with lower power requirements and longer ranges. In addition to larger surface areas, nanomaterials offer enhanced absorption capacity and chemical reactivity, making them powerful decontaminants. Conventional solutions to the problem of decontamination use highly aggressive chemicals. Given their absorptive capacities, nanoparticles such as carbon nanotubes can be developed to contain specific biochemical catalysts capable of performing decontamination without the use of aggressive chemicals.[57]

Conclusion

As nanotechnology advances, the field will continue to offer new and improved versions of existing products and potentially, also new applications for the WMD space. However, in the near term, the field of nanotechnology is more likely to assist in countering WMD threats rather than pose new and immediate risks for the WMD space.

---

[45] Tyler Koslow, "This Might Be the Strongest AND Lightest Material Ever Seen in 3D Printing," *3D Printing Industry,* 12 February 2016, <http://3dprintingindustry.com/news/66608-66608/>.

[46] David L. Chandler, "New Institute Will Accelerate Innovative Fibers and Fabrics," Massachusetts Institute of Technology News Office, 1 April 2016, <http://news.mit.edu/2016/national-public-private-institute-innovations-fibers-fabrics-0401>.

[47] Mike Guarrera, "Lightweight: How Much Is a Gallon of Fuel Worth?" *Nanocomp Technologies, Inc.*, 4 September 2014, <http://www.nanocomptech.com/blog/lightweight-a-gallon-of-fuel-worth.>

[48] Brett Brune, "The Global Yarns Race Is On," *Smart Manufacturing Magazine,* 11 July 2016, <http://advancedmanufacturing.org/global-yarns-race-is-on/>.

[49] Dexter Johnson, "Carbon Nanotube Yarns Could Replace Copper Windings in Electric Motors," *IEEE Spectrum,* 3 October 2014, <http://spectrum.ieee.org/nanoclast/semiconductors/nanotechnology/carbon-nanotube-yarns-set-to-replace-copper-windings-in-electric-motors>.

[50] National Nanotechnology Initiative, "Benefits and Applications," <https://www.nano.gov/you/nanotechnology-benefits>.

[51] National Science Foundation, "Market Report on Emerging Nanotechnology Now Available," Media Advisory 14-004*,* 25 February 2014, <https://www.nsf.gov/news/news_summ.jsp?cntn_id=130586>.

[52] Rajesh Singh and James W. Lillard, Jr., "Nanoparticle-Based Targeted Drug Delivery," *U.S. National Library of Medicine National Institutes of Health,* 7 January 2009, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3249419/>.

[53] National Research Council, *Emerging Cognitive Neuroscience and Related Technologies,* 2008, <https://www.nap.edu/catalog/12177/emerging-cognitive-neuroscience-and-related-technologies>. See also OPCW, *Report of the Scientific Advisory Board,* RC-3/DG.1, 29 October 2012, <https://www.opcw.org/fileadmin/OPCW/CSP/RC-3/en/rc3dg01_e_.pdf>.

[54] See Hammes, "Cheap Technology Will Change U.S. Tactical Dominance."

[55] T.X. Hammes, "The Future of Warfare: Small, Many vs. Few & Exquisite?" *War on the Rocks,* July 2014, <http://warontherocks.com/2014/07/the-future-of-warfare-small-many-smart-vs-few-exquisite/>.

[56] James Carafano and Andrew Gudgel, "Nanotechnology and National Security: Small Changes, Big Impact," The Heritage

Foundation, 21 September 2007, <http://www.heritage.org/defense/report/nanotechnology-and-national-security-small-changes-big-impact>.

[57] Manoj K. Ram and Ashok Kumar, "Decontamination Using Nanotechnology," Nanotechnology Education Research Center, University of South Florida, <http://www.ibrarian.net/navon/paper/CHAPTER_1_Decontamination_Using_Nanotechnology.pdf?paperid=19334348>.

Nuclear Technology

In contrast to emerging technologies, the wide range of nuclear technologies has been understood for many decades. Still, given their direct relevance for the WMD space, it is worth considering whether recent technological innovations might lead to unanticipated leaps forward in nuclear capabilities by states and create new risks and/or opportunities for the WMD space.

Technology Overview

Production of weapons-usable fissile material remains the primary barrier to developing nuclear weapons. Thus, the nuclear technologies of most concern for national security policymakers include nuclear reactors and processes for uranium enrichment and plutonium reprocessing, all of which can be used to produce weapons-usable nuclear material.

In the late 1990s and early 2000s, the nuclear industry anticipated a renaissance of nuclear power after decades of stagnation due to the Three Mile Island incident in 1979 and Chernobyl accident in 1986. However, the promised nuclear renaissance mostly fizzled out when the industry was confronted with high capital costs of new nuclear powerplants, low prices for natural gas, and the Fukushima accident in Japan in 2011, a chilling reminder of the risks of nuclear power.

Despite the many obstacles to a robust future for nuclear power around the world, there is again growing enthusiasm about the prospect of a second nuclear renaissance, signaled by new interest in advanced nuclear technologies and reactor construction in many countries, primarily in Asia.

Unlike emerging technologies, technological innovations in the nuclear field are generally not new ideas, but rather new interest in old technologies. Minor modifications to these old technologies might address longstanding barriers to growth in the nuclear power. Many of these technologies were developed decades ago but were not pursued commercially because the alternatives were more economically viable. The nuclear industry is taking a second look at them to explore if improving these known technologies could mitigate some of the risks of nuclear power, including safety, sustainability, efficiency, and cost.

All commercial-scale projects are based on conventional or evolutionary variants of operating reactors (light water reactors) except for the Russian BN-800 (sodium-cooled fast reactor), which is mostly fueled with highly enriched uranium (HEU). For example, to mitigate safety risks, engineers are revisiting nuclear reactors with passive systems, underground siting, and increased safety margins. To address the problem of high capital costs, the nuclear industry is developing small modular light-water reactors. In an attempt to increase efficiency, engineers are looking to raise the temperature of the coolant in reactors, which would increase the efficiency with which the reactor's heat output can be converted into electricity.

Notably, rekindled interest in advanced nuclear technologies is not focused on opportunities for reducing the proliferation risk of nuclear power. Many of the advanced nuclear technologies reduce risks in one area only to increase risk in another area—especially in nuclear proliferation.

In the event of a nuclear renaissance, expanded nuclear power is likely to create a need for greater uranium enrichment capacity and more interest in plutonium reprocessing. The increased production, storage, transport, and use of plutonium, uranium-233, and other weapons-usable material and their greater distribution around the world raise the risk not only of greater proliferation at the state level, but also of nonstate actors acquiring the necessary material for an improvised nuclear device.

The Risks

Whereas many other emerging technologies have a great diversity of potential end users, nuclear reactors, uranium enrichment, and plutonium reprocessing are much more restricted in their legitimate application. Dual-use nuclear technologies can be used to generate nuclear power or radioisotopes or develop nuclear weapons, and any advanced nuclear technology that makes it easier to produce the requisite nuclear material for a bomb increases the risk of misuse of the technology by states and nonstate actors.

Increased production of weapons-usable material or material at higher levels of enrichment raises the proliferation risks of nuclear power. For example, some advanced reactors require enrichment greater than light-water reactors, which typically use 3–5 percet low-enriched uranium (LEU). Enriched uranium at this level would provide a good starting material for producing HEU for state actors seeking nuclear weapons. Plans for space exploration have renewed interest in fuels that are compact, light, and dense with energy. Although a norm has been established to minimize HEU applications for peaceful purposes, scientists may look to HEU as a solution for energy production in space.

A rise in the use of fast reactor systems would require additional plutonium reprocessing capacity, possibly leading to a wider distribution of fuel cycle facilities and separated plutonium. Advanced reprocessing technologies (aqueous reprocessing and pyro-reprocessing) are designed to produce higher purity plutonium to improve efficiency of energy production. This process would also make the plutonium more suitable for nuclear weapons.

Nuclear power has been greatly constrained by the high capital costs of building massive production capacity for urban settings. The nuclear industry is exploring small modular reactors with the vision of deploying a fleet of reactors, widely distributed to supply small remote communities and military bases. Greater mobility of small reactors and a wider distribution would increase targets of opportunity for sabotage and theft.

The nuclear industry is abuzz about molten-salt reactors, which may address some concerns about large amounts of nuclear waste but generate other safety and security problems. In a molten-salt reactor, the fissile fuel is dissolved in a circulating molten salt consisting of thorium-232, LEU, and fission products. Such reactors require "on-line" reprocessing of the fuel to remove fission products, making each unit both a reactor and a fuel-cycle facility. While reducing the volume of nuclear waste, these reactors produce bulk quantities of uranium-233, which is fissile material. In addition, the liquid form of the fuel increases the vulnerability of such reactors to sabotage.

Advanced laser enrichment also has garnered much attention of late. As soon as lasers were developed in the 1960s, scientists began looking for ways to use them to separate uranium-235 from uranium-238. The first technologies for laser isotope separation emerged in Livermore National Laboratory (AVLIS) and Los Alamos National Laboratory (MLIS). Less efficient for enriching uranium than gas centrifuges, neither of these technologies was commercialized.

Today, laser enrichment technology has experienced new life with the development of third-generation approaches.

The SILEX process, a third-generation technology, exploits the fact that uranium-235 and uranium-238 absorb different wavelengths of light. The uranium-235 in uranium hexafluoride gas is blasted with a laser, which causes the isotopes to reach a state of vibrational excitation and move out toward the outer rim of the gas. From there, the isotopes can be separated from the uranium-238.

In 2012, the Nuclear Regulatory Commission (NRC) granted a license to GE-Hitachi for construction and operation, thereby paving the way for first-ever commercialization of the technology. Progress toward a laser enrichment facility stalled in 2014 for several reasons, including the lack of demand for enriched uranium. With 12 countries producing enriched uranium using gas centrifuges, supply currently exceeds demand, keeping the price too low to make the enterprise sufficiently profitable.

Although the market has currently shifted away from third-generation laser enrichment, research is ongoing, and a spike in demand for enriched uranium could turn the table back in its favor. If commercialized, the technology may increase risk of proliferation by sparking enrichment programs. Compared to gas centrifuges, laser enrichment is extremely energy efficient and more compact, requiring a smaller facility footprint. The primary barrier to the technology is the availability of suitable lasers. Unlike gas centrifuge technology, which requires specialized knowledge, extensive expertise on lasers abounds in medical and telecommunications fields.

The Opportunities

In the nuclear field, some nuclear technologies could mitigate the risks associated with nuclear energy, including environmental risks and the potential spread of nuclear weapons. For example, advances in measurement technologies for nuclear materials would reduce the risk of diversion. The use of lasers in place of International Atomic Energy Agency environmental sampling processes would improve timeliness of detection of the presence of undeclared materials, serving as a deterrent for clandestine activities.

Fast reactors and molten-salt reactors are often touted for their ability to "burn" nuclear waste rather than to breed fissile material as other reactors do. In a conventional approach to breeding fissile materials, reusing the nuclear waste produced in a reactor requires spent fuel reprocessing, fuel fabrication, transportation, irradiation, additional reprocessing, and waste treatment. In contrast, molten-salt fueled reactors require “on-line” processing to remove the fission products. Thus, each unit is both a reactor and a bulk-handling fuel cycle facility. The additional fuel burn-up reduces the environmental risks associated with producing and storing nuclear waste.

Yet such closed fuel cycles produce huge quantities of separated plutonium that, if acquired by states or nonstate actors, could be used in a nuclear weapon. Moreover, the bulk amounts of material complicate the effectiveness of material accounting in that the windows of error are large enough to allow sufficient material for a bomb to pass through.

To address these risks, alternatives to conventional reprocessing that are more proliferation- and theft-resistant have received interest. PUREX reprocessing could be replaced by technologies that do not completely separate plutonium, but rather keep it mixed together with other actinides or fission products. However, the plutonium would not be significantly more difficult or hazardous to steal than separated plutonium and could be used to make a nuclear weapon, either directly or after minimal chemical processing.

Conclusion

Nuclear technology offers a useful contrast to the risks posed by emerging technologies in terms of its maturity, the limited and specialized audience for its legitimate applications, and the magnitude of consequences if the technology is misused. Notably, the U.S. Government and the NRC failed to holistically assess all of the risk factors of laser enrichment when it approved GE-Hitachi’s license application. The risk of nuclear proliferation was not a consideration in the decisionmaking process. This should be instructive when considering how to manage the risks posed by emerging technologies, which are changing daily and have unlimited peaceful applications.

Synthetic Biology

Synthetic biology creates new risks and opportunities for the WMD space that leverage new genome editing tools, growing collections of genomic data, and expansion of computing power. Advances in the life sciences can create new pathways for biological weapons development but at the same time will provide new capabilities for countering those weapons.

Technology Overview

Scientists have been altering the genetic code of plants and animals for thousands of years through the practice of husbandry. In the 1970s, scientists leveraged advances in recombinant DNA technology to take genetic code from one organism and insert it into another (cut and paste) to transform the plant or animal for the first time.

More recent advances in synthetic biology, specifically in the reading and writing of DNA and computer modeling, allow scientists to make sequences of DNA and living organisms from scratch, alter DNA of existing organisms, and potentially create entirely new organisms in the future.[58] Although synthesizing genetic material has been possible for decades, early techniques were extremely difficult and impractically time-intensive. Today, DNA synthesizers can produce genetic material of any sequence at a rapid speed.

Synthetic biology involves "the design and construction of new biological entities such as enzymes, genetic circuits, and cells, or the redesign of existing biological systems. Synthetic biology builds on the advances in molecular, cell, and systems biology and seeks to transform biology in the same way that synthesis transformed chemistry and integrated circuit design transformed computing."[59]

With recent advances in synthetic biology, we now have direct access to life's genetic code. All of life is encoded using DNA's four-letter alphabet (A, G, T, and C). DNA sequences made up of strings of letters are copied from nature and then produced synthetically using a DNA synthesizer. As a platform, biology is incredibly sophisticated, programmable, capable of manipulating matter at the nanoscale, and scalable to any mass. Synthetic biology can be used in several ways: as a tool for discovery (for example, understanding disease); to make new things, alter microbes and single cells, or create specialty cells, microbes, and materials, or to change existing organisms (plants, animals, and human beings).

To simplify the creation of new organisms or modify existing ones, scientists are identifying greater numbers of standard DNA sequences that code for certain functions. These can be used by scientists around the world to construct new genes and DNA sequences.

Gene editing tools such as CRISPR have made it easier, faster, and cheaper to modify genomes.[60] CRISPR is an acronym for Clustered Regularly Interspaced Short Palindromic Repeat. CRISPR refers to a cellular defense mechanism in bacteria involving proteins (Cas9) that have the ability to locate and cut strands of DNA at locations corresponding to specific genetic sequences. Technologies based on these mechanisms allow gene editing that is more precise, cheaper, and faster than any prior tools.

Along with easy-to-use and inexpensive gene editing tools, standard components and increasing information about the functions of certain gene sequences have helped to fuel the "democratization of science." The open nature of the life sciences and easy-to-use tools have lowered the requirement for tacit knowledge and reduced the costs for using advanced techniques in biology. A wider range of actors have easier access to both explicit and tacit knowledge, lowering the barriers to entry for some portions of the pathway to biological weapons development. Do-it-yourself open biology laboratories and the annual International Genetically Engineered Machine competition are examples of this trend.

Meanwhile, in academic and government labs, scientists and engineers are working with computer-aided design and modeling, which allows them to rewrite and reprogram entire genomes. Advances in this area are important for designing genomes of organisms engineered for specific purposes and large-scale production of biological products made from these organisms.

Biology is a strategic technology for the 21st century. Just as information technology and the Internet have transformed society, business, government, and warfare since the late 20th century, biotechnology will similarly shape the global landscape for the next several decades.

The locus of this economic innovation is in industry, and particularly startups. Government funding is just one of many factors shaping the trend.

In the United States, revenue from the biotechnology sector has grown more than 10 percent each year on average over the past decade.[61] In 2012, biotech revenues exceeded $324 billion, which amounts to more than 2 percent of U.S. gross domestic product, rivaling other critical sectors to the U.S. economy.

Applications of synthetic biology remain constrained, however, by the extent to which the underlying biological functions are understood. Biological systems are extremely complex, and the interactions among various different processes are not always understood sufficiently well to predict and/or design the behavior of systems with synthetic components. This limitation is mitigated by the ability to run a great many experiments in parallel, empirically identifying and then optimizing systems that have the desired properties. The rise of cyber espionage could serve as a further constraint to the development of synthetic biology. For example, Ginkgo Bioworks, a company that recently won an investment of $45 million, makes money out of creating "custom-made organisms" from digital genetic codes it has built. Protecting these codes from industrial espionage once they are incorporated in engineered organisms is extremely challenging because as the engineered organism is shipped out to clients, its genetic instruction code can be copied, costing millions in lost revenue.

The Risks

Synthetic biology will become increasingly available and possibly of greater interest to nefarious actors with malicious intent. The ability to circumvent traditional detection and countermeasures and increasing ease and access to technology will empower a diverse range of actors to investigate the feasibility of biological weapons. However, significant challenges remain—particularly in the areas of weaponization and dissemination—that will not be overcome solely through advancements of biotechnology.

State actors will leverage synthetic biology for military purposes that are not prohibited by the Biological Weapons Convention, and they may see opportunities or incentives to start, or restart, biological weapons programs. State actors will invest in biotechnology to improve warfighting capabilities such as enhanced human performance, adaptive materials and sensors, and so forth. These kinds of "legitimate" military uses of biotechnology could mask illegitimate programs. Militaries may see incentives and impetus to regenerate biological weapons programs if synthetic biology enables capabilities providing significant military advantages, such as masking detection, complicating attribution, and providing targeted and discriminate effects previously unattainable. For example, synthetic biology may enable intentional creation of new forms of biological weapons that include modifications or enhancements of traditional threats, novel threat agents, and genetically selective effects weapons.

Gene drives, a technique that promotes the inheritance of a particular gene to increase its prevalence in a population, can be enabled by emerging biotechnology. Gene drives may be subverted as disease dissemination tools or environmental or agricultural threats; and our lack of ability to detect them may also be a problem. We do not have a complete understanding of the potential impacts that gene editing technology may have when introducing engineered species into environments, yet we now have the capability to create engineered species that can change a wild-type population in the environment into an engineered one.[62] We do not have a good baseline for monitoring biological/ecological systems that would indicate when a harmful gene drive had been introduced.

Bioinformatics, the collection, storage, and analysis of biological information using computers, is a growing sector. Protection of genomic information is a critical biosecurity issue. An understanding of the underlying function of DNA and genomes is a key enabler of emerging biotechnology. Genome data for humans, animals, and plants will be crucial to the bioeconomy, national biodefense, and important health initiatives such as Precision Medicine. It will be key to leverage genomic data for best advantage to U.S. science, economy, and biodefense, while safeguarding against potential misuse and protecting group and individual privacy.

Convergence with other emerging technologies will further accelerate economic development and societal change. Emerging trends in nanotechnology, robotics, information technology, and other fields will impact biotechnology's advancement. For example, the industry is in the process of adopting automated manufacturing platforms (automated fermentation platforms, for example, and automated laboratory processes), which may pose additional vulnerabilities and biosecurity challenges.

Synthetic biology has increasingly converged with concepts related to 3D printing over the past few years in the growing field of bioprinting.[63] Synthetic biology allows for the reprogramming of cells to enhance or leverage particular desired pathways. Combined with 3D printing that can precisely place particular cell types at particular locations in a structure or material, synthetic biology has potential for highly predictive human cell- and tissue-based technologies that can be used for drug discovery, drug toxicity, environmental toxicology assays, and complex in vitro models of human development and diseases.

Organovo developed the first 3D bioprinter in 2009 for making human tissue and organs. To print an organ, scientists take a small piece of tissue from the patient's organ and then tease the tissue apart into its individual components. After a month of growing the cells in a lab, they are combined with a gel and fed into a printing cartridge. The tissue is then printed layer by layer to form a 3D shape.[64]

Bioprinters are still not capable of reproducing the complexity of living systems. Depending on how bioprinting advances in the future, this technology could conceivably be used with minimal tacit knowledge by state and nonstate actors to modify existing pathogens or develop novel pathogens designed to harm humans, animals, or plants. Recent developments in genetic engineering and genomic information have been published in open-source literature and could serve as blueprints for others. The starting materials and equipment are inexpensive to obtain.

The Opportunities

Synthetic biology is essential for addressing the global challenge of resource scarcity, providing unprecedented advances in public health and medicine and for creating innovative products that support national defense and stimulate the U.S. economy. Moreover, synthetic biology holds significant promise for new solutions and countermeasures for the WMD space. In fact, the tools of biotechnology itself are likely the best options for ensuring biodefense against misuse.

Synthetic biology will break new ground in the health sector and force protection, providing new approaches for disease treatment and prevention that take into account individual variability in genes, environment, and lifestyle for each person.[65] These advances will extend to the development of new medical countermeasures such as new vaccines, antibiotics, and treatments. Genome editing tools, which allow for the precise engineering of targeting, function, and control mechanisms, can be used to develop immune therapies or T cell therapies for use in treating HIV infection and cancer. As another example, the chemical countermeasures program at the Defense Threat Reduction Agency is leveraging the convergence between synthetic biology and nanotechnology to develop a targeted nanodelivery platform with a payload consisting of DNA plasmids coding for proteins active in scavenging nerve agents.

Applications of new technologies such as gene drives can counter disease vectors (such as mosquitoes and rodents) to prevent disease. Such technologies may also be applied to invasive species management, improving biodiversity.[66]

Synthetic biology is also being used to enhance sensing capabilities for WMD in which living organisms detect ionizing radiation or small changes in environments. Synthetic biology is producing new classes of inexpensive, rapidly deployable diagnostic devices, getting closer to the prospect of real-time surveillance of disease agents.

Synthetic biology may lead to direct improvements to the warfighter. Bio-inspired innovations (human performance enhancements, advanced materials, "living" sensors, and new forms of energy production) will enable new military capabilities that can alter current dynamics in military competition. Research and development of products for skin and gut microbiomes (probiotics) will lead to enhanced human performance.

Synthetic biology can also be used to make "specialty" materials such as corrosion-resistant coatings or high-strength polymers. For example, the U.S. Army is funding an effort at Utah State University to produce spider silk. By splicing genes from orb-weaving spiders and inserting them into goats, the goats produce spider silk protein in their milk. A single goat produces about an ounce of protein per milking session, yielding several thousand yards of a single spider-silk thread.[67] The milk proteins are separated and purified, washed, freeze-dried, and converted to powder form. The powder is spun into a fiber or used to make coatings or adhesives. Textiles made from silk are lighter and tougher than Kevlar and do not melt like nylon. In addition to armor, spider silk can be used for medical purposes.

Conclusion

Advances in synthetic biology produce great promise for health, the environment, the economy, and the WMD space. However, the dual-use problem long associated with biology will also become intensified. The rapid pace of change in synthetic biology far outpaces policy innovation, making risk mitigation extremely challenging for policymakers.

---

[58] Jay Bennett, "New Organisms with Synthetic DNS could lead to Entirely New Life Forms," *Popular Mechanics,* 24 January 2017, <http://www.popularmechanics.com/science/a24879/organisms-synthetic-dna-new-life-forms/>.

[59] As defined by SYNBERC, "What is Synthetic Biology?" *Engineering Biology Research Consortium,* <https://www.synberc.org/what-is-synbio>.

[60] Heidi Ledford, "CRISPR, the Disruptor," *Nature* 522 (4 June 2015): 20.

[61] Rob Carlson, "Estimating the Biotech Sector's Contribution to the U.S. Economy," *Nature Biotechnology* 43, no. 3 (March 2016): 247.

[62] Antonio Regalado, "We Have the Technology to Destroy all Zika Mosquitoes," *MIT Technology Review*, February 8, 2016, <https://www.technologyreview.com/s/600689/we-have-the-technology-to-destroy-all-zika-mosquitoes/>.

[63] Bioprinting is the use of computer-aided transfer processes for patterning and assembling living and non-living materials with a prescribed 2D or 3D organization in order to produce bio-engineered structures. See F. Guillemot, V. Mironov, and M. Nakamura, "Bioprinting Is Coming of Age," Report from the International Conference on Bioprinting, Biofabrication in Bordeaux, 2009, U.S. National Library of Medicine National Institutes of Health, 2 March 2010, <http://www.ncbi.nlm.nih.gov/pubmed/20811115>.

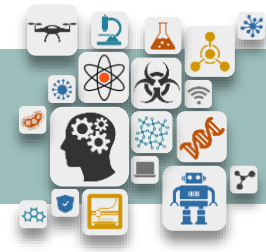
[64] "Changing the Shape of Medical Research and Practice," *Organovo,* updated 2017, <http://organovo.com/about/history/>.

[65] As defined by NIH, "About the Precision Medicine Initiative," <https://www.nih.gov/precision-medicine-initiative-cohort-program>.

[66] Kevin M. Esvelt et al., "Emerging Technology: Concerning RNA-guided Gene Drives for the Alteration of Wild Populations," *eLife,* 17 July 2014, <https://elifesciences.org/content/3/e03401>; James E. DiCarlo et al., "Safeguarding CRISPR-Cas9 Gene Drives in Yeast," *Nature Biotechnology* 33 (2015): 1250–1255.

[67] Sarah Kramer, "Genetically Engineered Spider Goats Could Be Biotechnology's Next Big Hit," *Business Insider,* 28 April 2016, <http://www.businessinsider.com/genetic-engineering-goats-spiders-2016-4>.

Governance Challenges



Over the course of several years, the Emergence and Convergence study at the WMD Center will examine the impact of emerging technologies on current tools and approaches for countering WMD and will explore the range of governance options for closing critical gaps. Emerging technologies present policymakers with a complex and inherently contradictory challenge of mitigating risk while simultaneously promoting innovation and economic growth.

The dual-use challenge is not a new one for the WMD space, but the unique features of emerging technologies make it far more difficult to devise meaningful governance mechanisms that reduce threats and avoid unintended consequences:

- Advances in emerging technologies are being primarily driven by the private sector and nonstate actors rather than governments.
- The rapid pace of change across all emerging technologies outpaces policy innovation and will make it harder to track those developments that enhance the capability to do harm.
- Numerous features of emerging technologies are reducing barriers to advanced capability and making them accessible to a wider variety of actors, making it difficult to conceive of any type of top-down governance measure that could be applied across the board to maximize benefit and minimize risk.
- The legitimate applications of emerging technologies are very broad and are used by many people, whereas those seeking legitimate applications of nuclear power are a relatively small set of actors who can all be identified and more feasibly placed under regulation.
- Many more people are doing legitimate things than illegitimate things, and it has become more difficult to distinguish between legitimate use and misuse.
- The digital nature of emerging technologies makes them harder to control than technologies whose spread depends primarily on physical objects.
- To the extent that "top-down" governance measures on emerging technologies are feasible, the window for implementing them before technologies become pervasive is likely to be more narrow than in the past, due in part to the fact that the technology is likely to diffuse more rapidly than in the past.
- Our current set of tools for countering WMD is not sufficient for addressing risks posed by emerging technologies that have strategic significance without creating "mass destruction."

Past experience with nuclear technology offers a useful contrast in terms of its maturity, the limited and specialized audience for its legitimate applications, and the magnitude of consequences if the technology is misused. Relatively speaking, control of nuclear technology should be more straightforward than the challenge of controlling emerging technologies. Nuclear technology was not developed first as a civilian technology; rather, it was a military technology that happened to have civilian applications. Despite its greater amenability, governance for the risk factors of nuclear technology consistently fail to be assessed in a holistic manner. The risk of nuclear proliferation has often not been decisive in the decisionmaking process.

Emerging technologies generally have very widespread civilian application, yet they may also have nefarious applications for states and nonstate actors. Any attempt to control emerging technologies like we control nuclear technology is destined for failure. Additionally, emerging technologies may provide the most effective solutions to countering WMD. Understandably, scientists and engineers fear that any talk about governance for emerging technologies will lead to draconian and highly damaging policies in which the prevention of possible misuse overwhelms all other concerns. Given the wealth of both benefits and risks these technologies pose that are unrelated to WMD, it is clear that the WMD paradigm for control is an inappropriate lens through which to view emerging technologies, but this begs the question about the right approach. While emerging technologies will challenge current nonproliferation regimes, WMD concerns should not drive the overall U.S. approach to emerging technologies, but should be considered in the context of a holistic policy.

To avoid unintended consequences of governance, risk assessments must drive to consideration of the range of policy solutions. The Emergence and Convergence study has launched a risk and opportunity assessment that will help to inform priorities and develop and compare different courses of action for addressing any gaps in countering WMD that are raised by emerging technologies. The study will conclude with a report on its findings, a menu of options for addressing the risks and opportunities produced by emerging technologies for the WMD space, and specific recommendations to policymakers for getting the most return on investment across the menu of options.

Graphic Credits: All graphics in the cover image are licensed under CC BY 2.0 and available from the Noun Project. Designers include Aaron K. Kim (robot), Bakunetsu Kaito (drone), To Uyen (DNA), Will Adams (3D printer), Christopher Holm-Hansen (security symbol), Rohith M S (chemical symbol), Delwar Hossain (biology), Maxim Kulikov (bacteria, microscope), Josy Dom Alexis (flask), unlimicon (laptop), Jeremie Sommet (microbe), Luca Reghellin (molecule), Gyan Lakhwani (nanoparticle), Wes Breazell (brain), Edward Boatman (wireless), and Rflor (biohazard).

NDU Press