Emergence & Convergence

Research Paper No. 4

October 2018

WMD in the Digital Age: Understanding the Impact of Emerging Technologies

Natasha E. Bajema

Dr. Natasha E. Bajema is a Senior Research Fellow at the Center for the Study of Weapons of Mass Destruction at the National Defense University. Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Defense Department or any other agency of the Federal Government.

Imagine a news headline flashing across the screen of your smartphone: "Terrorists deliver a biological weapon at a local sports stadium using drone swarm controlled via a smartphone, unleashing widespread panic and mass casualties." Upon further reading, the news article reveals an unidentified terrorist cell claimed credit for the attack. Law enforcement officials have determined the group purchased off-the-shelf drones from an online retailer, leveraged a free, open source swarming program to coordinate activity across the drones, and used a DNA desktop synthesizer to produce the genome of a dangerous pathogenic virus acquired online. The group claimed in an anonymous post that it managed to insert the virus DNA into a cell and scaled it up in a garage biolab. The terrorists left no evidence of their physical presence at the stadium or their identities and now remain at large. Law enforcement officials state they have no leads on the exact location from which the terrorists remotely launched their attack. They will need a team of cyber experts to help investigate the digital trails and pick up a trace. Although this news story is fictional, the potential for non-state actors to carry out such an incident already exists today.

For the purpose of this paper, emerging technologies are science-based innovations that empower small groups and individuals to acquire technologies that may rival capabilities of larger institutions. Technologies such as 3D printing, advanced robotics, synthetic biology, and nanotechnology are not only disrupting and transforming society and industry in profound ways, they are also disrupting how policymakers need to think about national security and countering weapons of mass destruction (WMD).[1] These technologies are lowering barriers to effective

development and use of WMD, creating new pathways for developing WMD, reducing the risk of detection of WMD activities, and offering nefarious actors new capabilities to cause mass effects. As such, they are altering the WMD space, both in terms of threats we face and our ability to counter them. In this new and rapidly changing threat environment, it is naïve to assume that states and non-state actors will develop and use WMD as they have done in the past. Although there are currently few direct links between emerging technologies and WMD, policymakers need to recognize that nefarious actors seeking to develop WMD in the future will leverage the asymmetric capabilities and competitive advantages available to them. The game is changing, and we need to adapt our mindset to meet these new challenges.

For more than two years, the WMD Center at National Defense University has been leading the charge with its multi-year study entitled Emergence and Convergence. This paper summarizes key initial findings about the impact of emerging technologies on WMD. In the Digital Age, there are three broad trends associated with emerging technologies that are fundamentally altering the WMD context, changing the threat space, and undermining the traditional tool box for countering WMD: these are digitization, convergence, and democratization. This paper will describe each of these trends, explore their implications for WMD threats, and illustrate how they undermine our current toolbox for countering WMD. The paper will conclude with recommendations for U.S. policymakers on important first steps to address these new national security challenges.

Digitization: From Atoms to Bits

Digitization, the conversion and movement of information between the physical and digital worlds, is the first major trend shaping the context for WMD, potentially leading to changes in how states and non-state actors develop and use WMD in the future. As both a product and a driver of the Digital Age, digitization provides the vital engine for the other two trends discussed in this paper: convergence and democratization.

For several decades, exponential growth in information and communication technology—a function of expanded capacity of microchips, falling costs of computing power and data storage, miniaturization of electronics, and the rise of the Internet connecting everything together—has produced the trend toward the digitization of everything. The importance of this trend may be on par with the invention of the printing press in the 1400s, a development that has been linked by scholars to several major periods of change in human history including the Renaissance, the Reformation, and the Enlightenment.[2] Similar to the Digital Age, the printing press led to major "increases in the ease and speed with which knowledge could be promulgated; feedback could be received and incorporated; one could find up-to-date knowledge and one could be put in touch with a wide range of materials on the topic."[3] It also "changed the conditions under which information was collected, stored, retrieved, criticized, discovered, and promoted."[4] Much time still needs to pass before we will know if the Digital Age matches or exceeds the impact of the printing press.

Digitization describes a process in which the physical and digital worlds are merging closer and closer together. Physical matter is

increasingly expressed as bits, converting the physical into digital.[5] The process of digitization began with the conversion of numbers to binary code consisting of 0's and 1's, to enable efficient data computation by computers. It was not until computers became connected to networks and later the Internet that the drive to digitize information expanded to text communications, images, audio, and video.[6] The outer limits of the potential for digitization seem uncertain at this time. These days, it seems like anything can potentially be expressed as digital code—e.g., the genomes of living organisms, home-made plastic guns, DIY drone designs, nuclear power plant parts, jet engine parts for commercial aircraft, missile parts, rolodexes of social connections, and even brain waves.

Coinciding with extraordinary growth in computing power, the trend toward digitization of information has been exponential, producing changes to society, business, and government that are difficult to fully comprehend even after several decades. In 1965, Gordon E. Moore, the founder of Intel, made a bold prediction. He noted that computing power had been doubling once a year, every year, since the development of the first prototype microchip. He predicted this trend would continue for the next decade.[7] As Moore predicted, computing power has doubled roughly every 18 to 24 months, leading to unprecedented exponential growth.[8] Aided by expanded bandwidth for transmitting information and the dropping cost of data storage, computing power has served as a forceful multiplier across all sectors of human and economic life—altering the incentives for digitizing new types of information and radically reducing the size of electronics.[9]

The irrevocable and seemingly unstoppable march of all things physical becoming digitized has vast implications for society, industry, and government. Klaus Schwab, chairman and founder of the World Economic Forum, and others have referred to the coming transformation as the Fourth Industrial Revolution—"characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres."[10] Digital information has gone from being merely a product of the Digital Age to becoming a powerful engine for transformation across all sectors due to its wide array of special characteristics—accessibility, speed, compression of time and space, lack of jurisdiction, and high commercial value.

To understand how digital information is transforming the WMD landscape, we must remind ourselves how fundamentally it has changed how we live our lives and conduct our daily business. Today, we can access an unimaginable volume of digital information from small, hand-held computing platforms—e.g., smartphones. With smart devices at our finger tips, we can seamlessly communicate with friends and family, get directions to almost any address on planet Earth, access our bank accounts and deposit checks, order merchandise and groceries from online retailers, track our steps and exercise, listen to music and audio books, read books and watch movies, play games, and even pay for our purchases at nearly any brick and mortar store. The list goes on and on.

Digital information offers unmatched convenience due to its incredible speed. Lacking color, size, or weight, digital information moves at the speed of light—or at least as fast as our current bandwidths will allow.[11] The effects of information speed are

most evident in the constant spinning of the 24/7 news cycle or when a social media post goes viral within hours, taking on a life of its own.[12] The news media has come under increasing pressure to respond to events in real-time, only seconds after they take place and to produce reliable information as they continue to evolve. This has led to an understandable reduction both in quality and depth of reporting, but it has also changed how facts are perceived. The speed and volume of digital information has blurred the notion of what information should be considered "fact" and contributed to the problem of fake news.

Smartphones have not only made our lives more convenient and productive by providing immediate access to the mobile Internet, they have changed the way we know, perceive, and interact with the physical world.[13] Digital information compresses both time and space, removing physical barriers to information of the past and altering the need for physical space to achieve certain ends.[14] In other words, we need less time to do things and often very little physical space to achieve them. Only two decades ago, to gain access to certain types of information, it was still necessary to visit a library, to search through a card catalog for journal articles and books manually referenced on note cards, and then to retrieve the books or journals from the shelves.

In the distant past, physical and time constraints were more extreme, requiring trips across oceans by boat. Today, we have immediate access to virtually unlimited and easily searchable and up-to-date information with a click of a button from our office chair. There's no time lag in gaining access to information or need to move to a physical location—it remains at our virtual finger tips, allowing for just-in-time learning.[15]

Now that smartphones and the Internet are vital parts of our daily lives, the trend toward digitization is self-reinforcing. The more we consume digital information and grow accustomed to its many conveniences for our daily lives, the more we demand quality digital information.[16] Digitization has enabled a common global language across diverse electronic platforms connected to the Internet. This feature has led to the networking of more physical objects over the Internet and around the world—often referred to as the Internet of Things.[17] When everything is digital, everything can be connected and move across the Internet and electronic platforms with ease. Since bits comingle effortlessly with each other, we can consume and leverage the same digital information on a growing range of smart devices.[18]

As access to digital information has become more convenient, new and daunting national security challenges have arisen for governments, companies, and individuals concerned with information security and integrity. Digital information has no jurisdiction or boundaries around it—although it is stored on physical devices and moves through physical systems, it is not itself physical. That means digital information is borderless, and unlike physical objects, it cannot be easily contained or controlled.[19] Once uploaded to the Internet, unencrypted digital information is potentially accessible to anyone with access to the Internet.[20]

Digitization is also shifting perceived value from physical objects to digital files. Digital information imposes fewer costs for reproduction and transmission than typical for

the physical realm. Manufacturers invest significant effort to produce each copy of a physical object and must outlay resources to transfer each produced item between locations—e.g., material costs, labor costs, and shipping.[21] Beyond the cost of storage and transmission of digital information, however, the transaction costs for reproducing and reusing digital files amount to zero. Most of its costs are attributed to its initial production in the first place.

Digitization has led to a glut of online data that promises to shape our world well into the future. Never before has the world produced such a significant volume, velocity, and variety of data that can be leveraged with analytical tools to detect behavior patterns and predict future outcomes.[22] Internet users, both human and machine, are constantly generating new data in real-time, doubling the total volume of existing data every year.[23] With every digital action, each one of us produces new data points—e.g., every email, text, and phone call, Internet download and click, camera selfie, eBook page reads, GPS input, automobile sensor, social medial post, credit card swipe, and store purchase—produces bits of data.[24] Smart devices, i.e., Internet-enabled, monitored and remotely controlled by human users, are also increasingly generating data from their internal operation processes or about their external environment using sensors, GPS, radio frequency identification (RFID) chips, etc.[25] As more smart devices are embedded with sensors and actuators, machines become capable of independently producing and exchanging data and of exerting effects in the physical world.[26] In other words, not only can physical matter be digitized, digital information can control the operations of machines that manipulate matter.

Digitization has produced a new body of knowledge and information products with substantial commercial value. Collections of digital information—i.e., large data sets referred to as big data—have become increasingly powerful and valuable as predictors of behavior. The concept of big data and its perceived value is not new. What has changed are the volumes and types of information that can be easily analyzed. In the early years of the Digital Age, companies leveraged big data solutions to analyze structured data (the type of data found in a traditional database) and organize and manage complex supply chains. Over time, increases in computing power and data storage capacities have allowed for more sophisticated models and data analytics that are capable of analyzing vast and untapped troves of digital information—most recently, a set of new cognitive and machine learning tools collectively referred to as artificial intelligence.[27]

Artificial intelligence promises to be the next major breakthrough for the analysis and use of digital information. With machine learning tools, companies and governments can now analyze larger volumes of data and a broader range of data types with greater complexity—e.g., unstructured data such as images, videos, documents, sensor/machine data, social media posts, and Internet clicks—to detect patterns and outliers, forecast trends, and perform cognitive tasks.[28] Unlike the rule-based algorithms of the past, machine learning algorithms are capable of learning rules and concepts from patterns found in massive data sets and developing solutions to problems.[29] These tools have the ability to perform functions on their own with limited human oversight. The breakthroughs in machine

learning tools were made possible by the massive volumes of "training data" generated as a result of several decades of data generation in the Digital Age.[30] The more data processed, the more refined and powerful the algorithms become.[31] Digital information is considered the new oil that will fuel the engine of artificial intelligence.[32]

Whereas the Digital Age provides the new context for WMD, digital information offers potential new pathways for the development of WMD and other weapons of mass effect. In the Digital Age, the context for WMD is changing rapidly. The first phase of transformation in the WMD space is arising from the digitization of a new "species" of emerging technologies.[33] As various elements of WMD programs become digitized, there will be several significant changes to the nature of the WMD threat and our ability to counter WMD.

Implications for WMD

To date, national security policymakers have treated the threat of WMD as a physical problem, largely separate from cyberspace and the trend toward digitization. For many decades, this made sense. Most of the technologies underlying WMD matured during the Cold War, long before the dawn of the computer age, and thus have yet to interact significantly with today's information and communication technology.[34] Moreover, during that period, the international community proscribed the development of WMD through an intricate web of treaties, export control regimes, and sanctions which greatly reduced the incentives for pursuing WMD and delegitimized such programs as part of a country's military strategy. As a result, these technologies, except for limited peaceful and defensive uses, fell out of favor among most members of the international community several decades before information became digitized.

Although the WMD problem has remained relatively insulated from the effects of the Digital Age, that is about to change. A wide range of emerging technologies with potential WMD applications have digital components and are interfaced with the Internet, facilitating easy transfer, and are capable of having physical impacts through digital pathways.[35] For example, drones offer a potential platform for the delivery of WMD. They contain operating software and hardware, transmit many types of data, and rely upon GPS for navigation. Additive manufacturing can be used to produce equipment and parts needed to develop WMD. 3D printers operate using specific software, can be networked and connected to the Internet, and produce physical objects from digital files that can be important to the production and dissemination of WMD. Biotechnology, the technology underlying biological weapons, is transforming from a discipline involving the physical manipulation, development, and production of microorganisms and related materials into a branch of information technology through sequencing, online databases of gene sequences and genetic information, the use of big data and bioinformatics.

Through interaction with a new "species" of emerging technologies, the WMD threat will increasingly exhibit digital elements, allowing actors new ways to develop WMD and avoid detection. State actors and non-state actors seeking to develop WMD are likely to view 3D printing and other digitized technologies as powerful tools in their toolbox. The following section will examine the specific implications for the WMD space.

(1) Increased Speed of and Access to Information

The most obvious effect of digitization is that everything moves faster and more effortlessly, including WMD proliferation, due to immediate and unprecedented access to digital information. As various elements of WMD programs become digitized, the corresponding access to and speed of information will alter proliferation dynamics, especially during times of conflict and periods of significant resource mobilization. Consider how early developments in nuclear physics in the late 1930s might have unfolded differently today.

In order to learn about the latest developments in their field, scientists in the early 20th century had to travel a few weeks by boat to attend overseas conferences or wait several months for the printing and distribution of scientific publications (which were often written in foreign languages). Consequently, it took a while for the news about nuclear fission to travel, slowing response times.

After the discovery of nuclear fission was confirmed by Otto Hahn and Lise Meitner in December 1938, several weeks passed before their findings appeared in the German scientific journal *Naturwissenschaften* and the British scientific journal *Nature*.[36] Even so, Danish scientist Niels Bohr helped spread the news about nuclear fission to top nuclear physicists at the Fifth Washington Conference on Theoretical Physics held in Washington D.C. in January 1939.[37] It took a few months, but the discovery of fission sent a ripple effect through the scientific community and may have led Nazi Germany to secure access to uranium ore stockpiles in occupied Czechoslovakia in April 1939. In today's world, news of such magnitude would have reached all corners of the world within the span of a single 24-hour news cycle.

The speed and fluidity of digital information has also impacted the ability to keep sensitive developments under wraps. To prevent Nazi Germany from advancing their nuclear bomb efforts, nuclear physicists worked to keep new findings about uranium secret at the expense of their careers.[38] This way, they hoped to keep the Germans from advancing their nuclear program—including knowledge of the advantages of using pure graphite over heavy water (expensive and subject to limited availability) as a moderator for the first uranium pile.[39] Unaware of the scientific breakthroughs related to graphite in the U.S., German scientists remained focused on gaining access to heavy water, a critical mistake that stalled their progress toward the bomb.[40]

Regardless of context, there are enormous pressures in the academic research community to be the first to publish scientific findings, including research that could potentially be misused by nefarious actors. However, the Digital Age has increased the ease of information dissemination and opportunities for using prepublication of results as placeholders. Any attempt to maintain secrecy about breakthroughs would cause deleterious effects on a scientist's career, allowing someone else to beat him or her to the punch. Keeping progress a secret would inevitably fail, especially if discoveries were made in an open setting such as a university. New developments can be accessed as soon as they become available online from any location in the world with Internet connectivity.[41]

Today, it is hard to fathom the physical and time constraints on access to information or the ability to suppress information in a decentralized academic context that existed in the lead up to the Manhattan Project. Even with the relative dearth of information and significant time lags, scientists were able to establish the basic scientific principles necessary for producing a nuclear bomb in an incredibly short timeframe. In the Digital Age, rising tensions and resource mobilization for conflict would likely interact with science and technology at much faster speeds, leading to weaponized developments in key areas such as synthetic biology, nanotechnology, and artificial intelligence.

This is an interesting and important lens through which to view recent developments in synthetic biology, which is rapidly transforming the life sciences into a branch of information technology. Gene sequencing involves the conversion of genes or entire genomes from living organisms into digital information that can be read, processed and analyzed by computers.[42] Over the past several years, scientists have responded to dramatic reductions in the cost of DNA sequencing and synthesis, computing power, and data storage by sequencing greater numbers of gene sequences and the genomes of living organisms. They have digitized this information for storage in online databases and analysis on computers.[43] Scientists from around the world can then leverage this growing volume of genomic data to construct new genes and DNA sequences of interest, and potentially create living organisms from scratch.[44] Rather than acquire physical samples, researchers can now search these online catalogues for sequences of interest and analyze the data and/or have them synthesized to work with them in a lab environment.[45]

This became possible already in 2002 when scientists created an active polio virus from scratch through chemical synthesis.[46] In 2010, J. Craig Venter's team became the first scientists to create a living organism from computer data. His team assembled a genome based on digitized DNA sequences, synthesized the DNA, inserted the artificial DNA into a bacterial cell, and life took over from there. The bacteria began to function, grow, and replicate.[47] More recently, scientists at the University of Alberta in Canada pieced together the genome of the horsepox virus with the stated purpose of helping to develop more effective vaccines for its close relative, the variola virus which causes smallpox. Over the course of six months, scientists ordered DNA sequences of the virus by mail, put them together, and synthesized the virus in the lab. The project cost about $100K, which is rather cheap by scientific standards.[48]

Recreating pathogens from digitized genomic data only scratches the surface of national security concern. Over the past several years, China has been buying up interest in sequencing companies and gobbling up large data collections of genomic data from around the world in a bid to become a DNA superpower.[49] Already in 2016, China owned more than half the world's capacity for gene sequencing. Some of this capacity resides in biomedical companies within the United States, presumably allowing access to genomic data for American citizens.[50] China has purchased interest in these companies to support its 15-year plan for precision medicine. Large data collections of genomic data and lifestyle data may help scientists identify potential sources of disease and ailments and then tailor medical treatments to each person's genetic makeup. There are other

more ominous ways these data collections can be used in a biological weapons program, and hence there is growing concern about China's actions.

(2) Embedded Expertise

Despite easy and quick access to information, the requirement for tacit knowledge continues to serve as an important barrier to nefarious actors seeking to develop and use WMD. Tacit knowledge is needed to accomplish those aspects of a complex technical process, such as many involved in the production of WMD, that are not readily communicated through published descriptions. It is typically acquired through a "master-apprentice relationship (learning by example) or acquired by a lengthy process of trial-and-error problem solving (learning by doing)... such knowledge tends to decay if it is not practiced on a regular basis."[51] After successfully creating synthetic bacteria in 2010, Craig Venter noted that "at each stage of the process, a team of highly skilled and experienced molecular biologists had to develop new methodologies, which could be made to work only through a lengthy process of trial and error."[52]

In the past, national security policymakers worried about potential for brain drain, i.e., the tacit knowledge related to WMD existing in the minds of underpaid scientists and engineers who might be persuaded to assist states or non-state actors in developing WMD.[53] Today, the barriers provided by the need for tacit knowledge are declining significantly. In the Digital Age, tacit knowledge has become increasingly embedded in a) digital build files for additive manufacturing machines, which can manufacture parts that skilled machinists would formerly have had to construct; b) push-button technologies arising from programmed protocols for automated machines, which can conduct laboratory experiments that formerly required humans; and c) technical demonstrations captured on video, all of which are easily transferred as digital information over the Internet.[54]

Leading manufacturers are turning to additive manufacturing to create digital designs in order to produce complex and customized parts and products and to help streamline supply chains.[55] As they continue to integrate 3D printers and related technologies into their operations, these firms are contributing to a growing body of embedded expertise in the form of digital build files. These files—designed, tested, and qualified by scientists and engineers—embed a certain level of technical expertise in digital form. This embedded expertise allows individuals without the requisite skills to produce parts or products by simply loading up a 3D printer with the required raw materials and then pressing the print button. Once a digital build file is created, most of the work has been done to produce a functioning part. Some of this digitized expertise may include sensitive build files for advanced weapons technology not otherwise available.

For example, the nuclear energy industry, known for its costly operations and limited economies of scale, is leveraging additive manufacturing to gain cost savings by producing custom parts on demand.[56] In 2014, Sellafield nuclear power plant in the UK decided to exploit 3D printing to support its decommissioning and disposal of nuclear waste.[57] The plant used a 3D scanner to capture the dimensions of a container for radioactive material, designed a digital model for a lid that would fit the container perfectly. Then they printed the lid, saving both time and money that would be required if they used traditional tooling. 3D printing allows

companies to design one-off solutions to solve nuclear-specific challenges while saving money, reducing part production times, and increasing safety.[58] The use of additive manufacturing has quickly caught on across the global nuclear energy sector and has even begun to transform existing nuclear weapons programs.[59]

In the past, specific expertise and skills were required to translate a nuclear weapon design into a finished product using advanced manufacturing tools such as lathes or computer numerical controlled (CNC) machines. Current nuclear weapon states are turning to additive manufacturing to achieve efficiencies in producing weapons components. In the U.S., the Kansas City Plant manufactures non-nuclear components for the U.S. nuclear weapons program. In 2015, the plant began using 3D printing to design and produce non-nuclear components to reduce costs and the weight of parts.[60] As the number and variety of relevant sensitive build files expands over time, nefarious actors who gain access to them may be able to utilize advanced technologies, including those important to nuclear weapons, and in this way circumvent the need for experienced engineers and scientists with specific skillsets.

In addition to digital build files, a number of desktop machines such as 3D printers, bioprinters, and DNA sequencers are leading to substantial de-skilling in fields that previously required years of tacit knowledge. De-skilling is defined as "the process of reducing the level of technical expertise or complexity of use required for successful employment."[61] At the push of a button, these new machines allow individuals with less expertise to achieve results comparable to highly educated scientists.[62] Although these machines do not yet eliminate the need for tacit knowledge, they are advancing rapidly in response to high demand, and some areas may approach push button technology in the near future.

For example, in 2018, scientists invented an easier, faster, and more accurate method for synthesizing DNA.[63] The new method could potentially lead to the development of desktop DNA printers for use in research labs. In the past, scientists either had to order DNA from specialized vendors, who had the ability to screen what was being ordered to see if it was likely intended for nefarious use, or they had to synthesize short sequences and assemble genes by stitching them together, a process that required much trial and error (i.e., tacit knowledge), time, and the use of toxic chemicals.[64] The new technique leverages an enzyme found in the immune system that has the ability to synthesize long strands of DNA. This would allow scientists to skip over the difficult process of piecing genes together and make it easier for them to engineer new living organisms; it might also evade one of the control mechanisms that is currently in place to help prevent synthetic DNA from being misused.

In recent years, tacit knowledge has also been embedded into standard genetic parts that code for specific functions as well as pre-built CRISPR kits, which simplify gene editing.[65] By using standard components and computer modeling, scientists with less expertise can build living organisms from scratch.[66] Meanwhile, CRISPR kits available for purchase online contain all the materials and equipment needed for a specific procedure. The "open-access biology" movement has allowed teams of high-school and college students to come together in Boston for the annual iGEM (International Genetic Engineered Machine)

competition since 2004. In 2017, more than 300 teams from around the world competed to design, build, test, and measure an original biological system using standard DNA sequences and current molecular biology techniques such as CRISPR-Cas9.[67] The aim of "open-access biology" is to "allow a wide range of non-experts to participate in biotechnological innovation."[68]

Despite the ease of use, Jonathan Tucker warned that "many biological parts have not been adequately characterized, so their activity varies depending on cell type or laboratory conditions…"[69] When inserted into a living organism, standard components may interact in complex ways and have unexpected effects.[70] Moreover, though easier and cheaper to use than past gene editing techniques, CRISPR may produce unintended effects, which would require further research and substantial tacit knowledge to overcome.[71]

Although the need for tacit knowledge appears to be on the decline as a result of digital build files and push button technology, there are some hands-on and sensory skills that will always require learning via visual demonstration and repetition.[72] Even here, however, the conditions for acquiring such knowledge are changing. In recent years, scientists have started transferring theses skills by producing video recordings of themselves conducting experiments and then uploading these to YouTube. Using a more sophisticated model, the Journal of Visualized Experiments has published over 8,000 professional videos of scientific experiments from laboratories around the world in order to improve education and change the conduct of science.[73] Many of these videos demonstrate techniques that cannot be effectively conveyed in writing, but can now be accessed through a subscription.[74]

Emerging technologies are reducing barriers to tacit knowledge related to WMD through embedded expertise. However, they do not do so in a uniform manner and affect some technologies more than others.[75] In other words, tacit knowledge may continue to serve as a barrier to the development of WMD in some areas. For example, DNA sequencing and synthesis have become easier and cheaper, greatly simplifying the creation of living organisms from scratch. However, converting that DNA into a viable virus requires additional expertise, with the degree of difficulty depending on the type of virus, and the process of inserting bacteria DNA into a living cell (i.e, booting), getting it to take, and then scaling up the synthetic organism in the laboratory is very challenging and requires a significant level of expertise.

(3) Changing Incentives for Proliferation

The first two digitization effects—access to and speed of information and embedded expertise—combined with the anonymity afforded by the Internet (and more effectively, the Dark Web) may change the incentives for proliferation by underpaid scientists and engineers. As discussed in the previous section, national security policymakers have often been concerned about the incentives of underpaid scientists and engineers for using their expertise to work for countries seeking to develop WMD and willing to pay top dollar.

The most famous example of a scientist leveraging and selling technical expertise was that of A.Q. Kahn who in 1975 stole physical copies of centrifuge blueprints from his employer, a subcontractor of URENCO in the Netherlands and a list of part suppliers, and

fled to his home country of Pakistan. Shortly upon his arrival, he began work on Pakistan's nuclear weapons program and focused most of his efforts on developing a uranium enrichment program. A.Q. Khan established a complex network to circumvent export controls by nuclear suppliers in order to acquire parts for Pakistan's nuclear weapons program. He later sold the extra parts along with expertise and blueprints to countries such as Iran, Libya and North Korea.

Futurist Chris Anderson aptly points out, "the process of making physical stuff has started to look more like the process of making digital stuff."[76] Scientists can leverage their WMD expertise to develop and sell digital blueprints and earn money for their intellectual property. As previously discussed, once a digital design file is complete, most of the work is done. Selling and transmitting additional copies of the digital file involves almost zero transaction costs when compared to producing, selling, and transporting physical parts. In other words, each additional copy of a digital file after covering original costs becomes pure profit. Moreover, if used correctly, the Dark Web offers an anonymous platform for selling and transmitting such knowledge and escaping detection. As a result, underpaid scientists and engineers may increasingly be incentivized to develop and sell digital blueprints for WMD-related parts.

(4) Reduced Signatures

To hide illegal activities, nefarious actors often establish complicated supply chains and procurement networks designed to discreetly acquire sensitive parts produced by unsuspecting manufacturers.[77] As a side effect of digitization, emerging technologies may enable better cover and more pathways for proliferation activities in the future, reducing the signatures of WMD programs. Consider the example of A.Q. Khan's illicit nuclear trade network and how things might unfold in the future.

In the 1980s, Khan began ordering parts to supply Pakistan's nuclear program from a known network of nuclear suppliers—often ordering double the number of parts he needed.[78] To disguise his efforts to acquire parts, Khan used an elaborate and widely distributed procurement network of suppliers, manufacturers, foreign trading companies, and transshipment points across several countries including Switzerland, the United Kingdom, the United Arab Emirates, Turkey, South Africa, and Malaysia.[79] Notably, Khan worked with manufacturing workshops in South Africa and Malaysia which imported the necessary metals, equipment and components and then produced finished parts. The final parts were disguised with fraudulent packaging and false end-user certificates.[80]

Khan's network began to unravel in 2003. The CIA successfully infiltrated a factory owned by Scomi Precision Engineering (SCOPE) in Malaysia and a key part of Khan's network for developing parts to support a uranium enrichment program. In August 2003, the intelligence community detected several containers of centrifuge parts loaded onto a vessel in Malaysia and tracked the shipment as it made its way to Dubai where the parts were disguised under the label of "used machinery" and transferred to a German-owned ship called the *BBC China*. With the authorization of the German government, the ship was diverted to a port in Italy where officials boarded the vessel and found centrifuge components destined for Libya in its cargo hold. This was considered to be the first success

of the Proliferation Security Initiative (PSI). Later, in an attempt to claim innocence, Scomi suggested the shipments contained 14 semi-finished components and the intended use of the parts was unclear.[81]

Now imagine Khan had access to 3D printing technology, which enables distributed manufacturing. In the past, proliferators required a stable physical space from which to develop the infrastructure for producing WMD-related materials (in Khan's case, large manufacturing facilities) and buy time to carry out operations. Compared to subtractive manufacturing, additive manufacturing technologies tend to be more compact and have a smaller footprint, requiring less electrical power and a smaller physical space, making proliferation activities less detectable.[82] Due to its small footprint and digital format, 3D printing affords easy access to time and space for proliferators. Although proliferators still require physical space, their options for finding a safe space will become more numerous and agile with 3D printing.

Using additive manufacturing, Khan could have ordered single parts, scanned them, and reproduced them in smaller workshops around the world. With such technology, proliferators can receive and send digital blueprints electronically from almost any size space with access to the Internet, a 3D printer, and raw materials.[83] Proliferators can receive additional shipments of materials and equipment at their doorstep delivered by a shipping company, print parts, and assemble components or run their procurement through a supplier network. Individual workshops dispersed globally could be instructed to produce specific parts that would later be brought together for assembly in a different location. If one location was compromised, the operation could simply move and shift activities to another existing location. All digital files would be transmitted by email and downloaded from the next location. Since there is no requirement for economies of scale or specific expertise, a single workshop could produce an unlimited variety of parts, masking the intended purpose.

3D printing will likely transform how nefarious actors view the physical world and this will change how they proliferate. As Chris Anderson suggests, "the more products become information, the more they can be treated as information: collaboratively created by anyone, shared globally online, remixed, reimagined, given away for free, or, if you choose, held secret."[84] To avoid detection, proliferators might even consider 3D-printing WMD-related lab equipment.[85] Despite growing volumes of off-the-shelf technologies relevant for WMD programs, nefarious actors may still prefer disguising their efforts and thus turn to 3D printing. ISIS recently used similar procurement strategies to A.Q. Khan to acquire parts for its drone program and set up a supply network consisting of as many as five businesses in three countries.[86] Although ISIS did not use 3D printing to support its drone program, it did resort to DIY approaches to modify drones with cheap add-on parts to allow for projectile drops. It does not require a stretch of the imagination to envision such groups leveraging 3D printing as a useful alternative to purchasing parts.

Digitization allows nefarious actors to move fluidly between the digital and physical worlds, leveraging the space that best achieves their objectives. In this way, they are able to circumvent efforts to counter WMD proliferation in unanticipated ways, sometimes leading to the opposite effect of the policy's intent. For example, PSI was created in 2003 to

facilitate international cooperation on the high seas related to the detection and interdiction of illicit trade networks. More than 100 countries have agreed to take measures to interdict proliferation transfers of WMD, delivery systems, and related materials as well as to share information and take specific action to prevent proliferation from their own territories. This initiative was intended to address a critical gap in efforts to counter WMD proliferation. However, PSI addresses a physical problem, not a digital one.

In the future, efforts to monitor the high seas for WMD may lead proliferators to turn to digital pathways because there is less risk of detection and interference. In some cases, it could even be cheaper than transporting physical goods around the globe.[87] Digitization means that actors no longer have to rely on physical movement to conduct proliferation activities. By moving back and forth between the physical and digital worlds, proliferators can cover their tracks more effectively.

Digital pathways facilitate reduced signatures and complicate verification of obligations under multilateral treaties and regimes. Although obligations under these instruments still apply to the digital realm, the ability of member states to enforce these obligations over their territories is diminished by digitization. States, find it difficult to control the transfer of digital information without undermining the openness of Internet, upon which the global economy now depends.

(5) Cyber-physical Interface

As a result of digitization, many emerging technologies are bridging the physical and digital worlds in new ways. The cyber-physical interface introduces a new set of risks that enable physical effects to occur over digital pathways. Digitization involves more than simply converting physical matter to bits, it also entails making physical objects smart or allowing systems to be remotely controlled over the Internet. As more electronic devices become smart (i.e., infused with sensors, computing chips, and wireless access), they not only consume and generate digital information, they are also exposed to a host of cyber-vulnerabilities that have plagued computing devices for decades.[88]

The most obvious effect of the cyber-physical interface is the potential theft of valuable digital information. Digital files are vulnerable to hacking, theft and interception and are much easier to copy, distribute, and pirate than physical objects. For example, bio-industrial companies use genomic data collections to identify gene sequences that produce viable consumer products.[89] Malicious actors that exploit cyber vulnerabilities can steal proprietary information (e.g., raw genomic data, as well as the data and algorithms arising from the data analytics). Once hackers steal this proprietary information, companies face the risk of losing their market edge to new competition.[90]

Sabotage of digital information and associated supply chains is another major concern. Additive manufacturing offers new opportunities for manipulating supply chains through the direct sabotage of digital build files, the insertion of malicious code into design software or printer firmware, and the conduct of cyberattacks against networks of 3D printers.[91]

As another example, many bio-industrial companies use specialized algorithms and computer analytics to assist in their research. These algorithms, which are often proprietary,

are directed towards very specific tasks. For example, a company like Ginkgo Bioworks uses proprietary algorithms on gene sequences to find better ways to produce compounds and proteins in engineered yeast cells. In this way, companies may optimize gene sequences that increase the production and enhance the stability of "specialty chemicals" and proteins. If this proprietary data were housed on network servers and connected to the Internet, a competitor could hack the network and tamper with the information or insert malicious code into the software, thus sabotaging a rival company. At a minimum, the sabotage of data would force the company to halt research and production until the problem could be corrected.[92]

Rather than building their own WMD, nefarious actors may seek to achieve equivalent effects by exploiting cyber-physical interfaces to perpetrate a cyberattack against a WMD-related facility. Industrial facilities including chemical plants, nuclear power plants, and other WMD-relevant facilities. Such facilities are often controlled via Supervisory Control and Data Acquisition (SCADA) systems. Over time, these systems have become increasingly connected to internal networks and the Internet to allow for remote alerts, monitoring, and control. Nefarious actors that gain access to such systems can cause disruption to services and/or physical destruction and harm from afar.[93] If successful, actors could exploit a cybercrime to cause mass effects. For example, the alleged sabotage incident at a pesticide plant in Bhopal led to nearly 4,000 deaths and many more injuries. Today, it may be possible to sabotage such a plant from afar, causing off-site consequences from a remote location.

Convergence: Blurring Technological Boundaries

Digitization has enabled technological convergence at an unprecedented pace and complexity. Today, more and more technological innovations are emerging and evolving within multiple disciplines and between different fields of knowledge.[94] Although a popular buzzword today, there is no real consensus on what technological "convergence" means, how, why, and when it occurs, or its broader implications for society, business or government.[95]

Some technologists claim that convergence has been around for several centuries and the pattern is simple and straightforward. From this perspective, the term refers to the intermingling or "converging" of different technologies that has always taken place over time. For them, convergence is defined as several different lines of technology coming together in a new application or domain—e.g., a smartphone.[96] Although this type of technological convergence has occurred across history, proponents of this view argue a wider range of potential functions and applications for a broad array of technologies makes this era of convergence special.[97]

Other technologists consider the speed, character, and depth of today's technological convergence to merit being called a new revolution within the fields of science and technology.[98] These experts define the concept as referring to the fusion of different fields into "convergent technologies" that come to share a common knowledge and technological base and generate new domains of technology or interdisciplinary fields—e.g., nanotechnology, synthetic biology, and advanced robotics.[99] Some

suggest that technological convergence has even led to a paradigm shift in the conduct of science itself, requiring the reorganization of the entire research enterprise.[100]

On its face, the drive toward convergence across disciplines represents yet another logical outgrowth of exponential advances in computing power, the Digital Age, and digitization. For example, the Human Genome Project, launched in 1990, leveraged computers, genetics, and sequencing technology with the goal of mapping the 3 billion base pairs in the human genome. By producing the first fully mapped human genome in 2003, the project helped launch the new fields of bioinformatics and genomics and contributed to the falling cost of gene sequencing, even faster than the rate of Moore's Law. Futurist Ray Kurzweil predicts that information technology will continue to "produce exponentially better tools in the future.[101] Such tools will not only accelerate convergence across disciplines, but also produce many new fields of inquiry the in process.

The origins of today's convergence, however, seem to go deeper than a simple response to advances in computing power. Rather, convergence involves a significant change in how scientific research is conducted in the first place.[102] For much of the 20th century, the advancement of new scientific knowledge took place within single disciplines and separate university departments.[103] Scientific progress emphasized depth within a single discipline rather than breadth across multiple disciplines. Those pursuing new knowledge within a field were expected to "learn a small thing very, very well."[104] This approach led to incremental, albeit significant growth in individual disciplines throughout the 20th century, but it neglected interdisciplinary areas of research.[105]

The desire to solve complex problems for the benefit of society led many scientists and engineers to move beyond the scientific traditions of the past.[106] To do so, they began to leverage the rapid advance of computing power, the development of models to simulate complex processes, the rise of digital information, and the emergence of the Internet—a useful platform for sharing information and enabling scientists to tackle more challenging problem sets.[107] Solutions to contested societal problems were not to be found within a single scientific discipline.[108] By definition, these problems required thought from multiple angles and technical disciplines to address the different pieces of the puzzle. As diverse perspectives came together, scientists and engineers developed "high-technology" approaches to complex problems.[109]

In the past, university departments and funding mechanisms were not structured to support this type of work. For this reason, scientists and engineers had to form new institutions and seek new sources of funding to sustain collaboration across disciplines.[110] They formed research groups that included experts from different backgrounds and a variety of disciplines coming together to solve complex problems.[111] As scientists and engineers began exploring new knowledge between and across disciplines, they developed unifying concepts across fields and integrated different scientific perspectives to form entirely new multi-disciplinary fields.[112]

As an example of convergent science, the field of nanotechnology borrows from biomedicine, information technology, chemistry, photonics, electronics, robotics, and

materials science.[113] Rather than simply having a multi-disciplinary character, however, the field of nanotechnology takes place at the intersection of disciplines, creating a new engineering paradigm focused on atoms and molecules.[114] Nanotechnology broadly enables and converges with all other technologies since all things "that consists of molecules can, in principle, be integrated with each other."[115] The boundaries between formerly separate disciplines have blurred and may someday disappear altogether.[116]

Implications for WMD

The emerging technologies that are currently interacting with WMD exhibit a high degree of convergence. This poses a direct challenge to the silos of excellence within government, academia, and elsewhere for countering WMD. The trend toward convergence requires us to take a closer look at complex technological linkages and their potential impact on WMD. Moreover, convergence places additional burdens on those responsible for forecasting and anticipating future scenarios involving WMD, new modes of causing mass effect, and new methods for circumventing efforts to counter WMD. The following section will examine the specific implications for the WMD space.

(1) Enablers of Enablers

Convergence requires us to think more broadly when it comes to potential WMD threats, to go beyond first-order enablers to look at enablers of enablers. Consider the fictional WMD-related scenario introduced at the beginning of this paper. The starting point for the hypothetical terrorist attack was the smartphone, but not in the way that most people would initially think—i.e., as the device that enabled the operator to control the drone from a distance. Rather, the scenario was enabled by the microelectronics package originally developed for smartphones, which now forms an integral part of off-the-shelf drones, a potential delivery platform for WMD and a new mode for causing mass effect.

Most of us take for granted that today's cellphones contain a vast array of tiny and powerful sensors that help make the phone smart—a result of miniaturization of electronics. To give smartphones their incredible multi-functionality, engineers had to find ways to make a wide variety of sensors smaller and smaller. Thanks to the huge demand for mobile devices and exponential increases in the amount of computing power that could be fit on a single chip, they were able to achieve the necessary economies of scale. With more than 2.5 billion smart phones currently in use around the world today, the falling costs of sensors has enabled many other astonishing developments, including affordable off-the-shelf drones that are capable of carrying WMD.

The impressive variety of sensors in a smartphone are designed detect slight changes in the environment and convert the information into signals, which are then processed by the phone's hardware and software and translated into instructions for the electronic device. For example, the accelerometer in smartphones measures acceleration and enables motion sensing. This sensor allows smartphones to track steps and informs the software which direction users are pointing the phones. Likewise, accelerometers determine the position and orientation of drones in flight and assist in navigation. Today's off-the-shelf drones would not be possible without the lightweight and cheap gyroscopes developed for smartphones to determine

orientation relative to the earth and keep the camera steady for high quality imaging.[117] The GPS receiver on a smartphone pinpoints the exact location of the user and offers step-by-step directions to any destination using different modes of transportation. Today, GPS still supports the navigation systems for most off-the-shelf drones. These drones are capable of producing real-time, high resolution imagery and video, engaging in continuous surveillance, inspection, data collection and monitoring, delivering of packages, cargo and pesticide, autonomously navigating the skies, and interacting with other electronic devices using swarming tactics.

In the next few years, drone manufacturers will continue to integrate rapid advances in the areas of materials, communications, guidance systems, information technology, and sensors into commercial and off-the-shelf platforms, resulting in enhanced capabilities for end users. Lighter and longer lasting batteries will lengthen flight times. New guidance systems will broaden access to spaces with diminished GPS or no signals. Machine learning will increase the autonomy of these platforms and allow for independent flight, targeting, and swarming. Each of these technologies will enhance the power of drone platforms. In other words, a major development in the technological sub-components of drones could generate massive leaps forward in their potential as delivery systems for WMD.

(2) Expect the Unexpected

Due to complex interactions and interdependencies, technological convergence produces unexpected combinations of technologies that can multiply impact in unanticipated ways.[118] The unpredictable nature of scientific discovery and innovation makes it more complicated to predict the emergence of technologies that will impact the WMD space and to forecast emerging threats. Moreover, technological progress is not likely to be consistent, undermining any predictions we may endeavor to make. As futurist Martin Ford suggests, "it often lurches forward and then pauses while new capabilities are assimilated into organizations and the foundation for the next period of rapid advance is established."[119] Progress in one enabling technology area may lead to sudden innovation in another.

An unpublished paper by Philipp Bleek and Cyrus Jabbari about microfluidics and nanofluidics offers a good example of how unexpected WMD-related developments could arise from converging technologies.[120] Microfluidics and nanofludics allow for the manipulation of small quantities of fluids at the micro and nano-scales to rapidly produce chemical reactions with greater control, purity, and yield. The authors note that these features combined with a smaller foot print have driven impressive growth in the field of microfluidics over the past few years and led to increased accessibility of the technology. Scientists have leveraged 3D printing for its on-demand production and complex designs to incorporate these fluidics in custom microreactors, which can be used to rapidly produce chemical reactions and enable chemistry not feasible in other ways. According to Bleek and Jabbari, these microreactors could support nefarious actors seeking to produce biological, chemical, or nuclear weapons.

(3) New Capabilities, New Tactics

Converging technologies may produce new and unexpected capabilities for state and non-state actors. Combined with new tactics, these actors may be able to challenge

adversaries with far greater capabilities and achieve new modes of attack. For example, ISIS took its adversaries by surprise by leveraging off-the-shelf drones modified to drop explosives on unsuspecting forces below.[121]

Non-state actors are not alone in the creative use of new capabilities and new tactics. State actors, with access to advanced military capabilities, have turned to emerging technologies to achieve desired effects. For example, Russia allegedly used a drone carrying a grenade to destroy an ammunition depot in the Ukraine near the Russian border. Ukraine servicemen extinguished the fire and recovered the remains of one thermite grenade.[122] More recently, Israeli forces used drones to deliver tear gas from the air in an effort to disperse Palestinian protesters.[123] These are fairly straightforward uses of drones and tactics. In a complex scenario, a state actor might consider mass producing drones using a small factory of 3D printers to avoid detection and loading them up with basic swarming technology. These drones could be delivered under the cover of a semi-truck, railway car, or shipping container to catch the adversary by surprise. This approach could provide the means for gaining asymmetric advantage over a stronger adversary.

(4) Value Neutrality

The starting points for developing WMD are respectively weapons-usable fissile material, toxic chemicals, and dangerous pathogens. These materials pose a clear-cut dual-use problem. Most WMD-related materials have legitimate and illegitimate uses, but the legitimate uses are fairly limited. All WMD-related materials are inherently dangerous and pose a direct security threat and therefore need to be controlled.

In contrast, emerging technologies are value neutral, meaning they "are neither good nor bad; they are just tools for the advancement of human agendas."[124] Unlike WMD, the platforms for emerging technologies—e.g., CRISPR, drones, 3D printers—are not inherently dangerous and do not pose a direct security risk. For example, the Ebola virus causes, a deadly disease, whether it has been developed for use on the battlefield or used to test therapeutics and protective clothing. In contrast, CRISPR can be used to edit the genes of a mosquito to prevent it from carrying the Zika virus, or it could be used to make a pathogen resistant to antibiotics.

The dual use problem is more complex because they are value-neutral prior to use.[125] In the past, national security policymakers have used capabilities as a key metric for making assumptions about the behavior of states and non-state actors. Unauthorized actors in possession of many WMD-related capabilities—e.g., the capability to produce fissile material or the possession of toxic chemicals or dangerous pathogens—would imply nefarious intent under certain conditions. For emerging technologies, there is no way to discern intent from capability. A scientist can use CRISPR techniques to prevent and/or cure disease, or use it make a pathogen more deadly. Owning a CRISPR kit is neutral in the United States. In the absence of clear indicators, intent may matter more than capability for bad actors planning to exploit emerging technologies to cause harm. This poses a new challenge to governments seeking to counter WMD and mitigate the risks of emerging technologies.

The broad applicability of emerging technologies adds another complication.

Convergent technologies such as additive manufacturing, advanced robotics, nanotechnology, and synthetic biology should be characterized as both multi-modal and dual-use technologies to distinguish them from past technology types. Whereas dual-use technologies have both legitimate and illegitimate applications, the range of legitimate applications for WMD-related materials had tended to be rather limited. Multi-modal technologies support a much wider range of legitimate across many sectors. For example, gene editing tools have the potential to produce textiles, biofuels, industrial liquids, agriculture, food products, medical research, medical countermeasures, and much more. Multi-modal technologies also blur the lines between legitimate and illegitimate applications in ways that defy the binary distinction inherent in the term "dual-use". For emerging technologies, the mode of use can occur in a gray area between legitimate and illegitimate. As in the past, gene editing techniques can produce unintended consequences for the ecosystem when used in conjunction with gene drives. With their broad accessibility, multi-modal technologies present difficulties to states seeking to control who uses the technology and for what purposes.

Emerging technologies span an infinitely wide range of applications when compared to WMD. Emerging technologies involve not only new risks, but also new opportunities for strengthening national security, for providing new solutions to countering WMD, and for bolstering the economy. Though drones offer a potential delivery system for WMD, the field of advanced robotics facilitates a wide range of hazardous missions such as detection, removal, and decontamination. Additive manufacturing can support the development of WMD programs, but it also can simplify logistics and supply chains for the Defense Department, allowing the military to print parts in the field--not to mention how the technology lowers distribution costs, allows for customized manufacturing for civilian producers, thereby improving their profitability and competitiveness.

As we consider how to mitigate the risks of emerging technologies, we must also consider how to encourage technological innovation and promote them as engines for driving economic growth. To become the global rule-setter, the United States must lead in these sectors. Hence, emerging technologies will place additional strain on multilateral instruments such as export controls. An export control group involves a voluntary agreement among states to prevent the transfer of sensitive, dual-use items to suspicious end users. By coordinating their export control policies, members work to prevent malicious actors from acquiring necessary technology through control lists. In addition to the challenges of preventing the digital transfer of emerging technologies, it will be difficult, if not impossible, to secure agreement among member countries to include WMD-relevant emerging technologies on control lists given their broad range of applications and positive benefits to society.

(5) Greater Number of Stakeholders

Technological convergence confounds the development of effective governance to mitigate the risk of emerging technologies at both the domestic and international levels by expanding the number of relevant stakeholders. In addition to requiring knowledge across multiple technical fields and disciplines, the decision-making authority related to converging technologies is widely dispersed across government agencies.[126] The

interagency landscape is complex for most national security issues. In the past, however, we could draw some useful boundaries. For the traditional WMD space, the relevant agencies that needed to come to the table to solve critical problems on WMD issues and make progress advancing a specific agenda were limited to a few key national security agencies with appropriate decision-making authority. For a convergent technology such as nanotechnology, the number of key stakeholders expands to more than 20 federal agencies with critical and divergent stakes, different authorities, and jurisdictions. This makes the development of governance more difficult than in the past.

(6) The Difficulty of Definitions

Whereas convergence complicates drawing clear boundaries among stakeholders, it also thwarts formulating specific definitions of emerging technologies. Moving forward on national security governance in these new areas requires defining the problem set and mission space for purpose of organizing meetings, programming, and budgets. The need for definitions is particularly profound at the multilateral level where broad definitions may provide sufficiently wide berth for states to disagree over whether a certain set of activities is in compliance with treaty obligations or not.

As an added hurdle, multilateral treaties and regimes rely upon consensus-based definitions. Without definitions, multilateral cooperation does not have a starting point and cannot move forward in an effective way. The fast pace of technological advancement, the multi-modal character of emerging technologies, and increasing convergence across multiple sectors will continue to complicate the chances of reaching agreement on definitions and hinder effective governance at the international level.

DEMOCRATIZATION: ADVANCED TECHNOLOGY FOR THE MASSES

Both digitization and technological convergence have propelled forward a third trend shaping the WMD space. The democratization of science and technology refers to the diffusion of power away from governments, big industry, and large organizations to much smaller entities such as startups, communities of citizen scientists and even individuals. These three trends are interacting in complex ways to change the nature of WMD threats and our ability to counter them. Although the trend of democratization has emerged alongside digitization and convergence, in many ways the scale of the democratization occurred as a direct consequence of them.

Digitization enables broad accessibility. Providing unprecedented access to information and a cheap forum for real-time communication and sharing of knowledge, the Internet has removed barriers and empowered individuals to make and do amazing things—for good or for bad purposes. Chris Anderson, founder of 3D Robotics, notes that "it used to be hard to change the world with an idea alone."[127] At the start of the Digital Age, computers began empowering people to create new ideas or intellectual property.[128] For an entirely digital operation, the cost of copying and transmitting the digital information amounts to nearly zero, lowering the barriers to production. Today, it has also become possible to prototype a physical product and sell it online without a massive investment in equipment, brick-and-mortar facilities, or economies of scale. Large

infrastructure, expensive upfront investments in tooling and equipment, and economies of scale are no longer necessary for production. In essence, the Internet has "democratized the tools of both invention and production."[129] The shift in power has led to the rise of DIY communities and makers who engage with emerging technologies and produce their own results.[130]

Advancements in information and communication technology have spurred rapid transformation and growth in technologies with digital components. Digitization has made these technologies easier to use through embedded expertise and de-skilling. Today, individuals with minimal skill can harness the capabilities embedded in computers and software, download instructions from YouTube videos, and create digital products, which can be transmitted in an instant to billions of people by simply clicking a button.

Technological convergence enables broad applicability of a single technology, allowing different domains to exploit economies of scale from other markets. As technologies achieve economies of scale more quickly through multi-functionality, prices drop, and this allows for further innovation. For example, the tiny and sophisticated sensors developed for the smartphone leveraged global economies of scale for communication devices. The growing demand for such sensors lowered the price and helped to launch the off-the-shelf drone industry as well as a wide range of other smart devices. Many of these sensors are now available for sale a low prices and can be integrated into other new inventions.

Today's emerging technologies are empowering individuals and breaking apart existing power structures by putting the tools of innovation, production, and distribution into hands of individuals and allowing them to achieve capabilities that rival those of large institutions.[131] The impact of a technology on society, industry, and government expands in response to its ubiquity or its democratization: "the more widely spread the greater the likelihood and magnitude of impact."[132] Due to the affordability and ease of use of emerging technologies, what was previously the sole domain of governments, large companies, and institutions has become the domain of individuals..[133] As a result, the private sector has assumed control from government as the dominant force in the arena of advanced technologies. With the private sector leading the charge in research and development, governments "no longer control research and development of cutting-edge technologies."[134] In essence, these technologies may be ushering "in a new world order."[135]

Implications for WMD

The trend of democratization yields significant benefits for society and economies around the world, but it also presents policymakers with a new, complex and dynamic national security challenge, requiring not only a shift in mindset, but also new approaches to mitigating future risks of WMD. In the past, the means of production for WMD-related materials and equipment were tightly held and controlled by a few large institutions in certain states. Until recently, the barriers to developing states non-state actors remained fairly restrictive. In contrast, the means of production for emerging technologies are broadly dispersed across the private sector, open source, participatory, and peer-driven.[136] Meanwhile,

governments are struggling to keep up with the speed of technological advancement. Lower barriers to entry are making increasingly powerful and WMD-relevant capabilities available to smaller and smaller entities. The following section will examine the specific implications for the WMD space.

(1) The DIY Marketplace

Lower barriers to advanced technology have led to the rise of DIY communities, which also serve as market drivers for technological advances in their respective sectors.[137] For example, industry experts hailed 3D printing as "manufacturing for the masses," predicting a near-term future that would involve households downloading digital files and manufacturing parts from desktop 3D printers.[138] 3D printers allow anyone to become a manufacturer with low entry level costs. Similarly, drones allow anyone to project power into the air and enable surveillance capabilities at increasing ranges, speeds, and durations from the comfort of their own backyards. Even more significant, in the place of experiments once conducted in laboratories, individuals can use a CRISPR gene editing kit for less than $200 to hack the genes of yeast or bacteria from the privacy of their garage.[139]

The DIYBio movement to make gene editing broadly accessible began in a garage.[140] Rob Carlson, a trained scientists and researcher, assembled a home lab from equipment purchased online with the aim of starting a new company. Afterwards, he published an article in *WIRED* magazine proclaiming the advent of garage biology. Around the same time, in 2008, Jason Bobe and Mackenzie Cowell launched the DIYbio.org message board and organized their first meeting at a pub near MIT. About 25 people turned up to the first meeting. Two years later, there were more than 2,000 subscribers.[141] Today a growing number of people around the world are doing biology as a hobby. This movement largely takes place within community labs and operates independently of government, academia and corporate institutions.

Similarly, a community of makers emerged around 3D printing. In 2006, Neil Gershenfeld at MIT's Center for Bits and Atoms launched the first Fab Lab to facilitate access to digital manufacturing technology: laser cutters, vinyl cutters, CNC machines, electronics, 3D printers, and machine shop tools. Individuals could use the lab space and equipment for free as long as they were willing to share their projects online.[142] At the time, 3D printers were still quite expensive. Today, there is a global network of over 1,000 fab labs and a wide array of affordable desktop machines.

Like the DIYBio and maker communities, there is also a thriving hobbyist community in the robotics space, driven in large part by the availability of open source hardware and software. The hobbyist drone community is dedicated to building their own drones and flying them with other hobbyists to hone their skills. The increased capabilities of off-the-shelf drones has led to the rise of professional drone racing and even the construction of stadiums to attend drone racing events.[143]

DIY communities represent a new economic force and a key driver for the advancement of emerging technologies. As hobbyists and citizen scientists place demands on the marketplace, companies will improve the capabilities of off-the-shelf capabilities, which are also available for purchase by nefarious actors will gradually increase.

(2) Made from Scratch

Emerging technologies are increasingly open source and shared online. Open source hardware, software, equipment, and materials allow individuals to easily construct their own 3D printer or drone at a fraction of the cost of off-the-shelf products. Open source technology also enables things to be made from scratch and away from government control.[144]

For example, a garage biolab can be set up for a few hundred to a few thousand dollars. To save on costs, biohackers have developed innovative workarounds for expensive lab equipment. For example, polymerase chain reaction (PCR) machines are essential for the study of genetics and capable of amplifying small amounts of DNA. These machines can be purchased from commercial suppliers, but they are expensive. To lower costs, biohacker Josh Perfetto created OpenPCR, which is an open hardware thermocyler.[145] It consists of a small plywood container with LCD screen. Inside the box, the device contains an Arduino processor board (open source electronics), a power supply, a container for DNA, enzymatic bath and heater coils. An OpenPCR costs $499 and can be modified for specific purposes.[146]

In addition to open source solutions for equipment, some DIYbio companies are producing pre-assembled kits to make genetic engineering more accessible. The Odin, led by biohacker Josiah Zayner, has created a frog kit that allows people to learn how to genetically modify animals and produce gene therapies. Frogs are genetically compatible with most human DNA gene therapies.[147] The kit includes everything needed to genetically modify the frogs to make them larger.

In the field of robotics, Stanford University's Artificial Intelligence Laboratory created the Robot Operating System (ROS) in the mid-2000s.[148] The idea was to create a free and open source operating system similar to Microsoft Windows that would form the basis for robotics innovation. ROS also offers open source modules for robotics simulation, movement, vision, navigation, perception, and facial recognition. Because the system is open source, skilled developers can modify it and enhance it. ROS has become the standard software platform for robotics development, lowering the barriers to entry. It is used by hobbyists and industry alike. For example, ROS powers the Baxter robot developed by Rethink Robotics, which enabled the company to offer if for far less than it would have otherwise.

Anyone with access to a computer, 3D printer, raw materials, and the Internet has the ability to create and share physical things in the comfort of their own home. The problem of 3D-printed plastic guns illustrates the potential of 3D printing for producing physical objects outside of control. In 2012, Cody Wilson, a second year law student at the University of Texas and his friends formed a group called "Distributed Defense" and launched a crowdfunding campaign to produce a 3D-printed plastic gun that could be made using a low-cost, open source 3D printer known as the RepRap.[149] In 2013, Defense Distributed successfully designed a plastic gun called "The Liberator" capable of firing a .22 caliber bullet and uploaded the design to a website.

The digital build file was downloaded about 100,000 times before the U.S. State Department intervened and ordered the blueprint to be taken down under the International Traffic in Arms Regulations (ITAR), which governs the export of munitions. Wilson took down the

blueprint, but it soon became available on other websites outside of U.S. jurisdiction. As an unintended consequence of the State Department's crackdown, the movement to 3D print plastic guns went underground and led to "the creation of an anonymized community using decentralized, encrypted, computer-aided designs."[150] This development makes it even more difficult for governments to monitor activities, let alone regulate them.

In 2015, Cody Wilson and Defense Distributed filed a law suit against the State Department, claiming his First Amendment rights were being infringed.[151] The State Department recently settled with Wilson, allowing Defense Distributed to release the designs online for downloading. In August 2018, however, a federal judge in Seattle granted a temporary restraining order to stop the posting of blueprints that would have legally allowed Americans to make 3D-printed guns in their own homes.[152] As of the writing of this paper, Defense Distributed has been ordered to remove its blueprints for 3D-printed guns from the Internet. Notably, the company is still offering for sale an open source CNC mill for $250 called the Ghost Gunner, designed to produce the lower receivers of AR-15 semi-automatic weapons. No prior experience is required to manufacture these parts from the design files. This open source technology allows individuals to manufacture rifles and pistols without serial numbers from their homes.

Open source technology allows individuals to make things away from government control. To mitigate the risks posed by emerging technologies, governments will have to wrestle with the challenge of controlling technology made from scratch and potential unintended consequences of regulatory measures.

(3) Intervention Points

In an era of garage biology, multilateral treaties and regimes are facing new and critical challenges to their effectiveness. The traditional tools and approaches developed over many decades to prevent WMD proliferation and to control WMD-related materials and equipment—e.g., nonproliferation treaties and export controls—were not designed to address risks associated with emerging technologies, nor are they equipped to do so moving forward.

Nonproliferation regimes consist of complex and interrelated webs of multilateral and bilateral agreements and activities designed to prohibit the development of WMD and regulate WMD-related materials, equipment and technology. A multilateral treaty requires years of negotiation, is difficult to amend, and faces significant constraints in adapting to new and emerging threats. These approaches are top-down by nature, have stabilizing effects, and primarily target the behavior of states and functioned fairly well during the bipolar structure of the Cold War.

By the end of the Cold War, however, the nonproliferation regimes already confronted significant challenges not only to their efficacy for regulating state behavior, but also to their capacity for addressing WMD emerging threats and non-state actors. Aside from inherent weaknesses in the treaty structures (e.g., lack of universality, verification) and difficulties with managing the non-compliance of member states, the regimes struggled in the 1990s to cope with the growing dual-use problem, exacerbated by globalization and the spread of technology.

In the early 2000s, policymakers attempted to extend the capacity of these tools to mitigate

the non-state actor problem by pushing for domestic implementation of the nonproliferation regimes with UN security resolution 1540. The resolution required all UN member states to adopt legislation to criminalize WMD-related activities and measures to prevent WMD terrorism such as export controls, minimum levels of physical protection on WMD-related materials, border controls, and transport regulations.

These modifications do not address the fundamental problem for governance posed by emerging technologies. Due to their broad accessibility and ease of use, emerging technologies have shifted the intervention point—i.e., the point at which a policy has regulatory effects—from states or technology manufacturers all the way downstream to the individuals within states. Not only does this pose a new requirement to domestic governments controlling activities within their jurisdictions, it places additional pressures on multilateral treaties for mandating a uniform national approach to the problem of WMD across countries. Individual countries will likely have to first solve the domestic problems posed by emerging technologies within the specific parameters of their legislative systems before addressing such challenges at the multilateral level.

The first attempt by the U.S. government to regulate operation of off-the-shelf drones by individuals provides a useful example. In 2016, the Federal Aviation Administration (FAA) issued the "small drone rule" for hobbyist and non-commercial drones weighing between 0.55 and 55 pounds. For a fee of five dollars, drone operators were required to register their drone with the FAA. Upon registration, drone operators receive an identification number to be affixed to the registered drone and are required to adhere to a list of flight restrictions including not flying drones over people, not engaging in beyond line of sight operations, not flying after sunset, etc. Commercial operators could apply for exemptions to these rules, which required certification as a remote pilot. In addition to FAA regulations, there are a myriad of state and local laws that apply to specific locations.[153]

From the perspective of mitigating the use of drones for causing harm, there are several problems with this approach to regulation. First, nefarious actors are unlikely to register their drones. In other words, this regulation will be ignored any anyone wishing to operate drones to cause harm. That does not negate the value of drone registration as it can be useful in distinguishing between good actors and those with potentially bad intent. Second, when a drone is in the air, there is no way for law enforcement officials to determine who the drone is registered to. Third, in the absence of training or viable options for bringing down a drone safely, law enforcement officials may be limited in what they can do about a problematic drone in flight. Given the challenges at the domestic level, it is hard to imagine countries coming together to cooperate at the multilateral level beyond an exchange of best practices.

(4) Conveyers of Norms

As a further complication to multilateral cooperation, states may no longer be appropriate or effective conveyers of norms moving forward.[154] In the face of accessible and easy-to-use emerging technologies, managing state behavior is no longer sufficient for mitigating the risks of WMD. Moreover, today's emerging technologies are not so easily controlled by states. However, this assertion goes beyond their ability to

effectively regulate or control technology. Multilateral treaties have played an important role in establishing norms against certain behavior. This made sense when WMD-related technologies were the province of states. Today, governments no longer dominate the development of advanced technologies; this has now become the realm of the private sector. As such, governments may not have sufficient understanding to mitigate risks without stifling innovation, or even legitimacy to determine best practices for behavior without direct input from private sector stakeholders. Even if states were to agree to certain obligations at the multilateral level, they may not actually have the ability to effectively regulate the technology within their own territory. Effective multilateral cooperation in the future may need to include key stakeholders in the private sector.

CONCLUSION

For several years, national security policymakers have been facing increasing pressure to grapple with the challenge of harnessing emerging technologies to deliver the greatest benefits to society, while safeguarding against their potentially malicious use. The WMD threat is no longer purely a physical problem, it is rapidly becoming a digital one. At the same time, forecasting emerging threats is more difficult as a result of the blurring of technological boundaries. With broad accessibility and ease of use associated with today's emerging technologies, the governance approaches to counter WMD in the past are losing their effectiveness. Emerging technologies are not only disrupting and displacing major industries and transforming society, but they are also disrupting established national security policies and governance structures designed to protect the public against harm from WMD. And so, it would appear that we are standing at a critical juncture of change.

In the absence of new ideas for governance to counter threats posed by the interaction of emerging technologies with WMD, it is tempting to apply the same types of governance or control mechanisms used in the past for preventing proliferation of WMD and other advanced military technologies. However, this strategy is not only doomed to fail, but it will also damage the U.S. position as a market leader and place significant restraints on what are vital engines of the future U.S. economy. For this reason, policymakers need to move beyond notions of control and consider a paradigm shift in how they view the threat of WMD, how they counter threats posed by WMD, and possibly how they define WMD itself.

We will not be able to develop a new toolbox for countering WMD overnight. Such an effort will require agreement from leadership at the highest level of government and a coordinated effort to define the new problem set, create new solutions, and divide up the relevant authorities. Engagement with and buy-in from key non-governmental stakeholders developing, affected by, or using these technologies will also be required. That said, there are a few things policymakers could do now to prepare for the looming changes to the WMD space.

First, it is time to reconsider our silos of excellence between WMD and cyberspace. Through interaction with a new "species" of emerging technologies, the WMD threat will increasingly exhibit digital elements, allowing actors new ways to develop WMD and avoid detection. State actors and non-state actors seeking to develop WMD are likely to view

digitized technologies as powerful tools in their toolbox. Policymakers should thoughtfully consider how to integrate cyber expertise into efforts to counter WMD.

Second, policymakers should consider increasing investments in horizon scanning and forecasting and make such products available across the government. Technological convergence places additional burdens on those responsible for forecasting and anticipating future scenarios. Often this complex analysis occurs outside of the communities that monitor WMD programs. Moreover, since the closure of the Office of Technology Assessment (OTA), U.S. Congress lacks the technical expertise perform effective oversight or to develop effective legislation to assess and/or mitigate the risks of emerging technologies. Better access to information about the cutting edge of emerging technologies will strengthen programs designed to counter WMD.

Finally, policymakers should explore the value of public-private partnerships for addressing the governance challenges arising from emerging technologies. While the private sector dominates the fields of emerging technologies, governments are struggling to keep up with the speed of technological advancement. Many government agencies—e.g., such as U.S. Special Operations Command/SOFWERX, the U.S. Air Force/AFWERX and the U.S. Army/Army Futures Command—are creating new structures that facilitate public-private partnerships. Policymakers responsible for countering WMD may be able to derive lessons learned that may apply to their own enterprise.

About the Author

Dr. Natasha E. Bajema joined the Center for the Study of Weapons of Mass Destruction at National Defense University in October 2008. Dr. Bajema currently is a Senior Research Fellow, the principal investigator for Emergence and Convergence, and Course Director for an elective entitled Through the Film-maker's Lens: Contemporary Issues in Combating Weapons of Mass Destruction and conducts research on global threat reduction programs. From 2010 to 2013, Dr. Bajema held a long-term detail assignment serving in various capacities in the Office of the Secretary of Defense, Acquisitions, Technology and Logistics, Nuclear, Chemical and Biological Defense Programs and in Defense Nuclear Nonproliferation at Department of Energy's National Nuclear Security Administration. The author is indebted to the following individuals for their reviews and insightful comments on earlier drafts of this paper: John Caves, Jerry Epstein, Diane DiEuliis, and Yong-Bee Lim.

Emergence & Convergence Study

In its multi-year study entitled *Emergence and Convergence*, the WMD Center is exploring the risks, opportunities, and governance challenges for countering WMD introduced by a diverse range of emerging technologies. The WMD Center identified advanced robotics as one of several emerging technologies for deeper assessment. 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 non-state actors and then for evaluating the nature of that impact on the current tools and approaches for countering WMD.

Dr. Natasha E. Bajema, Senior Research Fellow is the principal investigator for the study. The Emergence and Convergence study is supported by several offices within the Office of Secretary of Defense (OSD) and receives its primary funding from the CWMD Systems Program Office within the Office of the Assistant Secretary of Defense for Nuclear, Chemical and Biological Defense Programs/Threat Reduction and Arms Control (NCB/TRAC/CWMD Systems). The support by Mr. Jim Stokes, Director, CWMD Systems Program, has been critical to the project's success.

---

[1] George S., Day, Paul J. H. Schoemaker, and Robert E. Gunther, *Wharton on managing emerging technologies*, Hoboken, N.J.: Wiley, 2002, 2.

[2] James A. Dewar, *The Information Age and the Printing Press,* P-8014, Washington D.C.: RAND, 1998. Available at https://www.rand.org/pubs/papers/P8014/index2.html#fn0; Jeremiah Dittmar, "Information technology and economic change: The impact of the printing press," *VOX CEPR,* 11 February 2011, Available at https://voxeu.org/article/information-technology-and-economic-change-impact-printing-press

[3] See Dewar.

[4] Ibid.

[5] See for example, Nicholas Negroponte, *Being Digital*, New York: Vintage Books, 2000; Marc Goodman, *Future Crimes*, Transworld, 2016, 51.

[6] Negroponte, 4; See also Chris Anderson, *Makers: The New Industrial Revolution,* New York: Crown Business, 2012, 40.

[7] Joel Garreau, *Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies -- and What It Means to Be Human*, New York: Broadway Books, 2013, 49.

[8] Ibid.

[9] Ibid, 59.

[10] Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond," *World Economic Forum,* 14 January 2016, Available at https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

[11] See Negroponte, 14.

[12] For an important treatment of this topic, see P. W. Singer and Emerson T. Brooking, *Likewar: The Weaponization of Social Media*, Boston: Houghton Mifflin Harcourt, 2018.

[13] James Manyika et al, *Disruptive technologies: Advances that will transform life, business, and the global economy*, McKinsey Global Institute, May 2013, 6. Available at https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies

[14] Wilson Center, "Interview with Aude Olivia," *Leading Scientists Discuss Converging Technologies,* November 2014, Available at https://youtu.be/vZPveygyS4Q

[15] Ibid.

[16] See Manyika et al, 32.

[17] Ibid, 52.

[18] Negroponte, 18.

[19] John Perry Barlow, "The Economy of Ideas," *Wired,* March 1994, Available at https://www.wired.com/1994/03/economy-ideas/

[20] Negroponte, 4.

[21] Anderson, 107.

[22] Bill Briggs et al, *Tech Trends 2017: The kinetic enterprise,* Deloitte University Press, 2017, 36. Avaliable at https://www2.deloitte.com/content/dam/insights/us/articles/3468_TechTrends2017/DUP_TechTrends2017.pdf

[23] Briggs et al, 36.

[24] Goodman, 105.

[25] Manyika et al, 52.

[26] IEEE, *Artificial Intelligence and Machine Learning Applied to Cybersecurity,* 6-8 October 2017, 2. Available at https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/industry/ieee_confluence_report.pdf?utm_source=lp-link-text&utm_medium=industry&utm_campaign=confluence-paper

[27] Briggs et al, 35.

[28] Ibid, 21-23.

[29] Paul Scharre and Michael C. Horowitz, *Artificial Intelligence: What Every Policymaker Needs to Know,* Washington D.C.: CNAS, 2018, 4. Available at https://s3.amazonaws.com/files.cnas.org/documents/CNAS_AI_FINAL-v2.pdf?mtime=20180619100112

[30] Scharre and Horowitz, 5-6.

[31] Manyika et al, 42.

[32] Scharre and Horowitz, 5.

[33] See Jennifer J. Snow, *Entering the Matrix: The Challenge of Regulating Radical Leveling Technologies,* Monterey: Naval Post Graduate School, 2015, 5. Available at https://core.ac.uk/download/pdf/36739949.pdf

[34] First generation chemical warfare agents were developed as industrial chemicals in the 1800s and used for the first time on the battlefield in WWI. Second and third generation nerve agents were discovered in the 1930s and 1940s. Biological and nuclear weapons were first developed by governments during WWII. WMD programs underwent further incremental development throughout the Cold War.

[35] Snow, 5; Manyika et al, 14.

[36] Otto Hahn and Fritz Strassman's work was published in *Naturwissenschaften* on 6 January 1939. Lise Meitner and Otto Frisch's work was published a month later. "Disintegration of Uranium by Neutrons: A New Type of Nuclear Reaction" in the journal Nature on Feb. 11, 1939

[37] See Atomic Heritage Foundation, "Niels Bohr Announces the Discovery of Fission," Available at https://www.atomicheritage.org/article/niels-bohr-announces-discovery-fission

[38] Richard Rhodes, *The Making of the Atomic Bomb,* New York: Simon & Schuster, 1986, 345.

[39] Herbert L. Anderson, "The Legacy of Fermi and Szilard," *The Bulletin of Atomic Scientists,* Vol. XXX, No. 7 (Sept 1974), Available at https://library.ucsd.edu/dc/object/bb52575421/_1.pdf

[40] Simon Worrall, "Inside the Daring Mission that Thwarted a Nazi Atomic Bomb," *National Geographic,* 5 June 2016, Available at https://news.nationalgeographic.com/2016/06/winter-fortress-neal-bascomb-heroes-of-telemark-nazi-atomic-bomb-heavy-water/

[41] Jonathan B. Tucker, "Could Terrorists Exploit Synthetic Biology?" *The New Atlantis,* Spring 2011, 70. Available at https://www.thenewatlantis.com/publications/could-terrorists-exploit-synthetic-biology

[42] Natasha E. Bajema, Diane DiEuliis, Charles Lutes, and Yong-Bee Lim, *The Digitization of Biology: Understanding the New Risks and Implications for Governance,* Emergence & Convergence Research Paper Series No. 3, July 2018, Available at https://wmdcenter.ndu.edu/Publications/Publication-View/Article/1569559/the-digitization-of-biology-understanding-the-new-risks-and-implications-for-go/

[43] Bajema et al, *The Digitization of Biology.*

[44] Natasha E. Bajema and Diane DiEuliis, *Peril and Promise: Emerging Technologies and WMD,* Washington D.C., NDU Press, 2017. Available at https://wmdcenter.ndu.edu/Portals/97/Documents/Publications/Articles/2016%20Workshop%20Report%20FINAL%205-12-17.pdf?ver=2017-05-12-105811-853

[45] Bajema et al, *The Digitization of Biology.*

[46] J. Cello, AV Paul, and E. Wimmer, "Chemical Synthesis of Poliovirus cNDA: Generation of Infectious Virus in the Absence of Natural Template," *Science* 297 (2002), Available at https://www.ncbi.nlm.nih.gov/pubmed/12114528

[47] Bajema et al, *The Digitization of Biology.*

[48] Bajema et al, *The Digitization of Biology.*

[49] David Cyranoski, "China's Bid to be a DNA superpower," *Nature,* 22 June 2016, Available at https://www.nature.com/news/china-s-bid-to-be-a-dna-superpower-1.20121

[50] David J. Lynch, "Biotechnology: the US-China dispute over genetic data," *Financial Times,* 31 July 2017, Available at https://www.ft.com/content/245a7c60-6880-11e7-9a66-93fb352ba1fe

[51] Tucker, 70.

[52] Tucker, 71.

[53] John A. Lauder, "Statement for the Record on the Worldwide WMD Threat," Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction, 29 April 1999, Available athttps://www.cia.gov/news-information/speeches-testimony/1999/lauder_speech_042999.html

[54] Clare Scott, "Experiment Tests the Suitability of 3D Printing Materials for Creating Lab Equipment, *3Dprint.com,* 3 August 2018, Available at https://3dprint.com/221403/3d-printing-materials-lab/

[55] World Nuclear News, "Digitization Experts Explain Benefits for Nuclear," 5 July 2017, Available at http://www.world-nuclear-news.org/C-Digitisation-experts-explain-benefits-for-nuclear-05071701.html

[56] Wyatt Hoffman and Tristan Volpe, *An Internet of Nuclear Things: Emerging Technology and the Future of Supply Chain Security,* Stanley Foundation Policy Analysis Brief, June 2018, 2. Available at https://www.stanleyfoundation.org/publications/pab/IoNTPAB618.pdf

[57] Oliver Gomez, "3D Printing to the Rescue of Nuclear Power Plant," *3Dprintingpin.com,* 16 May 2014, Available at http://www.3dprintingpin.com/3d-printing-to-the-rescue-of-nuclear-power-plant/

[58] See for example, Jennifer J. Snow, "Acknowledging the Dark Side: Why Speaking Openly about Technology Threat Vectors is the Right Answer," in *Strategic Latency: Red, White, and Blue: Managing the National and International Security Consequences of Disruptive Technologies* edited by Zachary S. Davis and Michael Nacht, Center for Global Security Research, Lawrence Livermore National Laboratory, February 2018, Available at https://cgsr.llnl.gov/content/assets/docs/STATEGIC_LATENCY_Book-WEB.pdf

[59] In 2015, the DOE's Kansas City Nuclear Weapons Plant for manufacture of non-nuclear components is using 3D printing to prototype fixtures. See Tyler Koslow, "Keeping Nuclear Weapons Secure with 3D Printing at the National Security Campus, *3Dprintingindustry.com,* 28 October 2015, Available at https://3dprintingindustry.com/news/keeping-nuclear-weapons-secure-with-3d-printing-60927/. Siemens

[60] See Koslow.

[61] Snow, *Entering the Matrix,* 26.

[62] Snow, "Acknowledging the Dark Side."

[63] University of California – Berkeley, "New DNA Synthesis Technique Promises Rapid, High-Fidelity DNA Printing," *rdmag.com,* 19 June 2018, Available at https://www.rdmag.com/news/2018/06/new-dna-synthesis-technique-promises-rapid-high-fidelity-dna-printing

[64] University of California – Berkeley, "New DNA Synthesis Technique Promises Rapid, High-Fidelity DNA Printing."

[65] Snow, "Acknowledging the Dark Side."

[66] Tucker, 74.

[67] Bajema et al, *The Digitization of Biology.*

[68] Todd Kuiken, "Governance: Learn from DIY Biologists," *Nature*, 9 March 2016, Available at https://www.nature.com/news/governance-learn-from-diy-biologists-1.19507

[69] Tucker, 74.

[70] Ibid.

[71] Sharon Begley, "Potential DNA Damage from CRISPR has been 'seriously underestimated,' study finds," *Statnews.com,* 16 July 2018, https://www.statnews.com/2018/07/16/crispr-potential-dna-damage-underestimated/

[72] Tucker, 70.

[73] JoVE creates the ultimate solutions for advancing research and science education by making and publishing videos of scientific experiments from the top laboratories around the globe. See https://www.jove.com/journal

[74] Tucker, 71.

[75] Ibid, 78.

[76] Anderson, 25.

[77] David Albright, Paul Brannan, and Andrea Scheel Stricker, "Detecting and Disrupting Illicit Nuclear Trade after A.Q. Khan," *The Washington Quarterly,* April 2010, 89. Available at https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/130828_Detecting%20and%20Disrupting%20Nuclear%20Trade.pdf

[78] William J. Broad, David E. Sanger, and Raymond Bonner, "A Tale of Nuclear Proliferation: How Pakistani Built His Network" *New York Times* 12 February 2004, Available at https://www.nytimes.com/2004/02/12/world/a-tale-of-nuclear-proliferation-how-pakistani-built-his-network.html

[79] David Albright and Corey Hinderstein, "Unraveling the A.Q. Khan and Future Proliferation Networks," *The Washington Quarterly,* Spring 2005, 114. Available at https://www.tandfonline.com/doi/abs/10.1162/0163660053295176?needAccess=true#aHR0cHM6Ly93d3cudGFuZGZvbmxpbmUuY29tL2RvaS9wZGYvMTAuMTE2Mi8wMTYzNjYwMDUzMjk1MTc2P25lZWRBY2Nlc3M9dHJ1ZUBAQDA=

[80] Albright and Hinderstein, 115.

[81] Broad, Sanger, and Bonner.

[82] Deven Desai and Gerard Magliocca, "Patents, Meet Napster: 3D Printing and the Digitization of Things," *The Georgetown Law Journal,* Vol. 102 (2014): 1693. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2338067

[83] Digital blueprints do not include post-print finishing and assembly. However, a digital build file could come with instructions for finishing and assembly.

[84] Anderson, 72-73.

[85] Clare Scott, "Experiment Tests Suitability."

[86] Don Rassler, *The Islamic State and Drones: Supply, Scale, and Future Threats,* Combating Terrorism Center, West Point, July 2018. Available at https://ctc.usma.edu/app/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf

[87] Snow, *Entering the Matrix,* 5.

[88] Hoffman and Volpe, 2. See also Jean Peccoud et al, "Cyberbiosecurity: From Naïve Trust to Risk Awareness," *Trends in Biotechnology* Vol. 26, No. 1 (Jan 2018): 4-7; Randall Murch et al, "Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy," *Frontiers in Bioengineering and Biotechnology,* Vol. 6, No. 39 (Apr 2018): 1-6.

[89] Bajema et al, *The Digitization of Biology.*

[90] Brenda Goodman, "Agents Arrest 3 in Plot to Sell Coca-Cola Secrets to PepsiCo," *New York Times,* 6 July 2006, Available at https://www.nytimes.com/2006/07/06/business/06coke.html; Erin Ailworth, "Chinese Firm Found Guilty of Stealing Wind Technology From U.S. Supplier," *Wall Street Journal,*

24 January 2018, Available at https://www.wsj.com/articles/chinese-firm-found-guilty-of-stealing-wind-technology-from-u-s-supplier-1516829326

[91] Sofia Belikovetsky et al, *dr0wned: Cyber-Physical Attack with Additive Manfacturing*, Available at https://pdfs.semanticscholar.org/40de/144aee6e84d8638684133d0e48cce8ed67c9.pdf

[92] Bajema et al, *The Digitization of Biology*; see also, Randy Murch et al.

[93] Hoffman and Volpe, 3.

[94] Chie Hoon Song, David Elvers, and Jens Leker, "Anticipation of Converging Technology Areas," *Technological Forecasting & Social Change,* Vol. 116 (2017): 98. https://www.sciencedirect.com/science/article/pii/S0040162516305959

[95] Bryn Nelson, "Big Buzzword on Campus: Is "Convergence" a Revolution in Science or Simply Jargon?" *Scientific American,* 1 July 2011, Available at https://www.scientificamerican.com/article/big-buzzword-on-campus/

[96] Mihail C. Roco, "Possibilities for global governance of converging technologies," *Journal of Nanoparticle Research*, Vol. 10, No. 1 (2008): 2. Available at https://link.springer.com/article/10.1007/s11051-007-9269-8; see also Day and Schoemaker, 64-65.

[97] Kristin Alford, Sarah Keenihan, and Stephen McGrail, "The Complex Futures of Emerging Technologies," *Journal of Future Studies,* Vol. 16, No. 4 (2012): 68.

[98] For example, see *The Third Revolution: The Convergence of the Life Sciences, Physical Sciences, and Engineering,* White Paper, Massachusetts Institute of Technology, January 2011, Available at http://www.aplu.org/projects-and-initiatives/research-science-and-technology/hibar/resources/MITwhitepaper.pdf ; see also Wilson Center, "Interview with George Whitesides," *Leading Scientists Discuss Converging Technologies,* https://www.wilsoncenter.org/article/leading-scientists-discuss-converging-technologies-0 and James Gentile, "Is 'Convergence' the Next Revolution in Science," *The Blog,* Huffington Post, 11 December 2013, Available at https://www.huffingtonpost.com/james-m-gentile/convergence-science-research_b_4078211.html

[99] See Alfred Nordmann, *Converging Technologies: Shaping the Future of European Societies,* Report of the High Level Expert Group, 2004, 16, Available at https://www.philosophie.tu-darmstadt.de/media/institut_fuer_philosophie/diesunddas/nordmann/cteks.pdf; see also Song, 99; Day and Schoemaker, 64-65. MIT, *The Third Revolution*, 4.

[100] MIT, *The Third Revolution.*

[101] Nat Berman, "Three Technologies that Will Define Our Future According to Ray Kurzweil," *Money.Inc,* 2016, Available at https://moneyinc.com/three-technologies-will-define-future-according-ray-kurzweil/

[102] In a 2012 study called "Societal Convergence for Human Progress", the Wilson Center interviewed more than a dozen scientists working in the fields of nanotechnology, biotechnology, information technology and cognitive science in an effort to unpack the origins and meaning of technological convergence. https://www.wilsoncenter.org/article/leading-scientists-discuss-converging-technologies-0

[103] MIT, *The Third Revolution*, 5.

[104] Wilson Center, "Interview with George Whitesides," *Leading Scientists Discuss Converging Technologies,* https://www.wilsoncenter.org/article/leading-scientists-discuss-converging-technologies-0

[105] Wilson Center, "Interview with Paul Alivisatos," *Leading Scientists Discuss Converging Technologies*, https://www.wilsoncenter.org/article/leading-scientists-discuss-converging-technologies-0

[106] Roco, 2.

[107] Nordmann, 16; Alford, 74.

[108] Song, 98-99.

[109] See Interview with George Whitesides.

[110] MIT, *The Third Revolution.*, 9.

[111] See Interview with Paul Alivisatos.

[112] Roco, 2.

[113] Nordmann, 14.

[114] Wilson Center, "Interview with Mark Lundstrom," *Leading Scientists Discuss Converging Technologies,* https://www.wilsoncenter.org/article/leading-scientists-discuss-converging-technologies-0.

[115] Nordmann, 16.

[116] Tsjalling Swierstra, Marianne Boenink, B. Walhout, and R. Van Est, "Converging Technologies, Shifting Boundaries," *Nanoethics,* Vol. 3, No. 3 (2009): 213.

[117] Konstantin Kakaes, "What Drones Can Do and How They Can Do It," in *Drones and Aerial Observation: New Technologies for Property Rights, Human Rights, and Global Development,* edited by Konstantin Kakaes et al, New America, July 2015, 13. Available at http://www.rhinoresourcecenter.com/pdf_files/143/1438073140.pdf

[118] Manyika et al, 15.

[119] Martin Ford, *Rise of the Robots: Technology and the Threat of a Jobless Future*, New York: Basic Books, 2016, 64.

[120] Philipp C. Bleek and Cyrus Jabbari, *Honey, I Shrunk the Lab: Emerging Microfluidics Technology and its Implications for Chemical, Biological, and Nuclear Weapons,* Emergence & Convergence Research Paper Series No. 5, unpublished.

[121] Rassler, 1.

[122] Kyle Mizokami, "Kaboom! Russian Drone With Thermite Grenade Blows Up a Billion Dollars of Ukrainian Ammo," *Popular Mechanics,* 27 July 2017, Available at https://www.popularmechanics.com/military/weapons/news/a27511/russia-drone-thermite-grenade-ukraine-ammo/

[123] Nidal Al-Mughrabi, Jeffrey Heller, and Kelly-Ann Mills, "Israeli drones pour tear gas onto Palestinian protesters who used kites to fly petrol bombs over Gaza border," *Mirror,* 14 May 2018, Available at https://www.mirror.co.uk/news/world-news/israeli-drones-pour-tear-gas-12535483

[124] Zachary S. Davis, "Ghosts in the Machine: Defense Against Strategic Latency," in *Strategic Latency and World Power: How Technology is Changing Our Concepts of Security* edited by Zachary Davis, Ronald Lehman, and Michael Nacht, Center for Global Security Research, Lawrence Livermore National Laboratory, 2014, 25. Available at https://cgsr.llnl.gov/content/assets/docs/Strategic_Latency.pdf

[125] Ibid.

[126] Brian Holmes, "Strategic Latency, Technology Convergence, and the Important of the Weapons Mix, ," in *Strategic Latency: Red, White, and Blue: Managing the National and International Security Consequences of Disruptive Technologies* edited by Zachary S. Davis and Michael Nacht, Center for Global Security Research, Lawrence Livermore National Laboratory, February 2018, 264. Available at https://cgsr.llnl.gov/content/assets/docs/STATEGIC_LATENCY_Book-WEB.pdf

[127] Anderson, 5.

[128] Ibid, 14.

[129] Ibid 8.

[130] Jeremy Heimans and Henry Timms, "Understanding 'New Power,'" *Harvard Business Review*, December 2014, Available at https://hbr.org/2014/12/understanding-new-power

[131] Snow *Entering the Matrix*, 3. See also Albert Lin, "Herding Cats: Governing Distributed Innovation," *North Carolina Law Review* Vol. 96, No. 4 (2018): 947 and Heimans and Timms, "Understanding 'New Power.'"

[132] See Dewar.

[133] Mary Ellen Hannibal, "Democratizing Science," *Popular Science* 11 October 2016, Available at https://www.popsci.com/democratizing-science

[134] Davis, 22.

[135] Christopher Zember, "The Democratization of Science Ushers in a New World Order," *War on the Rocks,* April 2016, Available at https://warontherocks.com/2016/04/the-democratization-of-science-ushers-in-a-new-world-order/

[136] See Heimans and Timms.

[137] Snow, "Acknowledging the Dark Side."

[138] See for Example, Adrian Bowyer, "Manufacturing for the Masses," March 2017, Available at https://www.youtube.com/watch?v=yRM6cC-YtRw

[139] Loz Blain, "Do-it-yourself CRISPR genome editing kits bring genetic engineering to your kitchen bench," *New Atlas,* 12 November 2015, Available at http://newatlas.com/home-crispr-gene-editing-kit/40362/

[140] Rob Carlson, "Splice it Yourself," *Wired,* 5 January 2005, Available at https://www.wired.com/2005/05/splice-it-yourself/

[141] Heidi Ledford, "Garage biotech: Life hackers," *Nature,* 6 October 2010, Available at https://www.nature.com/news/2010/101006/full/467650a.html

[142] Anderson, 46.

[143] Ian Frazier, "The Trippy, High-Speed World of Drone Racing," *The New Yorker,* 5 February 2018, Available at https://www.newyorker.com/magazine/2018/02/05/the-trippy-high-speed-world-of-drone-racing

[144] John Hornick, *3D Printing will Rock the World,* 2015.

[145] See Open PCR at https://openpcr.org/

[146] Anderson, 221.

[147] Kristin Houser, "You Can Now Genetically Engineer Your Own Mutant Frogs for $499," *futurism.com,* 14 September 2018, https://futurism.com/mutant-frogs-genetic-engineering/; See the Odin's website at http://www.the-odin.com/frog-ge-kit/

[148] Read about ROS at http://www.ros.org/history/

[149] Marrian Zhou, "3D-printed gun controversy: everything you need to know," *cnet.com,* 25 September 2018, Available at https://www.cnet.com/news/the-3d-printed-gun-controversy-everything-you-need-to-know/

[150] Snow, "Acknowledging the Dark Side."

[151] See Zhou.

[152] Deanna Paul, "Federal Judge Blocks Publication of 3D-printed Gun Blueprints," *The Washington Post,* August 27, 2018, Available at https://www.washingtonpost.com/news/post-nation/wp/2018/08/21/federal-judge-will-soon-decide-whether-to-block-3-d-printed-gun-blueprints/?utm_term=.bac58d227b94

[153] Arthur Holland Michel, "Local and State Drone Laws," *Drones at Home,* March 2017, Center for the Study of the Drone, Bard Colleage, Available at http://dronecenter.bard.edu/state-and-local-drone-laws/

[154] Ashton Carter, *Shaping Disruptive Technological Change for Public Good,* Belfer Center, Harvard

University, August 2018, Available at https://www.belfercenter.org/publication/shaping-disruptive-technological-change-public-good