Gregory D. Koblentz

Emerging Technologies and the Future of CBRN Terrorism

As part of a nuclear security summit in 2016, fifty world leaders participated in a crisis simulation of a radiological terrorist attack. According to the scenario, the radiological material was stolen from a hospital and sold via the Dark Web to a terrorist group that delivered it using a drone against a civilian target.[1] The scenario, while fictional, was firmly rooted in technological developments that present a new range of challenges to preventing non-state actors from acquiring and using chemical, biological, radiological, and nuclear (CBRN) weapons.

Drones and the Dark Web are just two examples of increasingly available and capable emerging technologies such as malware, synthetic biology, 3D printing, artificial intelligence, robotics, the Internet of Things, autonomous vehicles, digital currency, nanotechnology, and genome editing.[2] The growing integration of these emerging technologies into our economies and societies led the World Economic Forum to declare in 2015 that we are witnessing the beginning of the Fourth Industrial Revolution.[3] This new era is characterized by its global scope, an exponential rate of innovation, and the convergence of the physical, digital, and biological worlds. The Fourth Industrial Revolution has the potential to

Gregory D. Koblentz is an Associate Professor and Director of the Biodefense Graduate Program at the Schar School of Policy and Government at George Mason University. He is also a member of the Scientists Working Group on Biological and Chemical Security at the Center for Arms Control and Non-Proliferation. He can be reached at gkoblent@gmu.edu. This article is derived from a paper presented to the UN Security Council on August 23, 2016 during its open debate on UN Security Council Resolution 1540 and the non-proliferation of weapons of mass destruction.

The Washington Quarterly • 43:2 pp. 177–196
https://doi.org/10.1080/0163660X.2020.1770969

transform entire systems of production, management, and governance with huge anticipated gains in productivity and prosperity.

But the Fourth Industrial Revolution also has a dark side: the scientific breakthroughs and new technologies that are fueling this new industrial revolution can be misused by non-state actors for malign purposes. According to Klaus Schwab, founder and chairman of the World Economic Forum, "As this process takes place and new technologies such as autonomous or biological weapons become easier to use, individuals and small groups will increasingly join states in being capable of causing mass harm. This new vulnerability will lead to new fears."[4] It would be far preferable to predict how these emerging technologies could be misused and take steps to minimize those risks ahead of time rather than to react after they are used to cause harm on a large scale.

This article will provide a brief overview of five of these technologies and discuss the ways in which they could be misused by non-state actors. Despite their fundamental differences, these technologies share seven characteristics that make them particularly worrisome. These seven characteristics are key to understanding the factors driving advances in science and technology, the likely trajectory of these emerging technologies, their assimilation by different segments of society, and the impact that these technologies can have on the risks posed by the proliferation of CBRN weapons to non-state actors. The article concludes with recommendations for how to strengthen international efforts to prevent the misuse of these emerging technologies by non-state actors.

Five Emerging Technologies of Concern

Among emerging technologies, five warrant special consideration for CBRN weapons.

Among emerging technologies, five warrant special consideration for their potential to increase the risk of non-state actors acquiring and using CBRN weapons: drones, the Dark Web, malware, synthetic biology, and 3D printing. There are already signs of drones, the Dark Web, and malware being misused in ways that increase the risk of CBRN terrorism, while synthetic biology and 3D printing pose longer-term risks.

Drones

Unmanned aerial vehicles (UAVs), or drones, are no longer so expensive and sophisticated that their use is restricted to a handful of states. The global market for commercial and consumer UAVs is expanding rapidly and is expected to

grow to over US$10 billion a year by 2025.[5] The proliferation of these types of UAVs has been driven in large part by the trillion-dollar smartphone industry, which pioneered the miniaturization of many of the components now found in drones: high megapixel cameras, long-lasting lithium batteries, high-precision GPS units, and the built-in sensors and high-speed processors needed for a reliable autopilot.[6]

UAVs provide non-state actors with unprecedented means of gathering intelligence and attacking targets in unconventional ways. They allow insurgents and terrorist groups to covertly gather intelligence on high-security areas by circumventing ground-based physical defenses, loitering for long periods of time, and providing high-quality imagery that could provide insights into a facility's layout and security measures. At least three terrorist groups—Hezbollah, Hamas, and the Islamic State—have used UAVs to collect intelligence on their adversaries.[7] There have already been several cases of anonymous operators using drones to collect intelligence on sensitive nuclear sites including nuclear reactors in France and a strategic nuclear weapon facility in the United States.[8]

A growing number of terrorist groups, including Hezbollah, Hamas, the Islamic State, and Palestinian Islamic Jihad, have weaponized commercial drones by turning them into flying improvised explosive devices (IEDs) or equipping them to drop small explosive munitions.[9] The Houthis in Yemen have also used weaponized drones provided by Iran to attack a variety of military and civilian targets in Saudi Arabia.[10] These attacks are even more worrisome when delivered by swarms of drones, which can approach a target from multiple directions and overwhelm defenders. In 2018, an unidentified rebel group repeatedly used swarms of armed drones, sometimes a dozen at a time, to attack Russia's airbase at Khmeimim in Syria.[11] In September 2019, the Houthis in Yemen claimed credit for an attack with almost twenty drones that knocked out the Abqaiq oil facility in Saudi Arabia, the world's largest oil refinery, although the attack is believed to have been conducted by Iran.[12]

While the explosive payload of a UAV is much less than that of a car bomb, weaponized drones have the advantage of being able to fly over physical barriers to attack targets inside of secure compounds. A camera-equipped drone would also allow the operator to aim at specific targets within a facility. These targets could include nuclear power plants, spent fuel storage facilities, chemical production and storage plants, shipments of highly toxic industrial chemicals, or high biocontainment laboratories. The locations of these targets are generally well known, and their defenses are optimized for repelling traditional terrestrial threats, not aerial assaults from above. Although such facilities are typically equipped with redundant safety systems, the use of drone swarms that could simultaneously target multiple sensitive points at a facility poses an additional security challenge.

Finally, UAVs could one day be used to deliver a weapon of mass destruction. Nuclear weapons will remain too large and heavy for delivery by the type of UAV that a non-state actor could build or buy, but other types of CBRN weapons could be delivered by drones. The small-payload, low-speed, and low-altitude flight profile of UAVs make them well suited for delivering chemical and biological agents against civilian targets.[13] A crop-spraying drone designed for use in the developing world can carry twenty liters of pesticides—or sarin.[14] By comparison, the Japanese cult Aum Shinrikyo killed eleven and injured more than 1,000 commuters when they released only six to seven liters of sarin in the Tokyo subway system in March 1995.[15] In April 2015, an anti-nuclear activist used a drone to deliver a small quantity of slightly radioactive soil to the roof of the Japanese Prime Minister's office.[16] While this incident was ultimately a harmless political gesture, it highlighted the diversity of payloads that drones can deliver and demonstrated the vulnerability of government buildings to attacks from above. The advent of UAVs optimized for carrying cargo, such as those being pioneered by Amazon and DHL, will create more opportunities to turn commercially available devices into flying IEDs or CBRN delivery systems with increased range and payload. At that point, a drone's payload capacity will be less of a limitation than the ingenuity of its users.

Nuclear weapons will remain too large but other CBRN weapons could be delivered by drones.

The Dark Web

The Dark Web is a restricted part of the internet that can only be accessed using encryption software, such as Tor, that guarantees anonymity to its users. Tor is used by a variety of non-state actors who wish to communicate securely over the internet, including dissidents, whistleblowers, criminals, and terrorists. The Dark Web also hosts numerous markets that offer a range of illegal goods for sale including drugs, guns, and pornography.[17] Most of these markets rely on the digital currency Bitcoin, a peer-to-peer transaction system that does not rely on central banks or the traditional financial system.[18] Since all Bitcoin transactions are encrypted to provide anonymity to both the buyer and seller, this digital currency poses special challenges for anti-money laundering, counterterrorism financing, and proliferation financing.[19]

The Dark Web provides terrorists interested in acquiring CBRN weapons with a new pathway for obtaining dual-use equipment or materials. The threat of CBRN terrorism has long been limited by the disconnect between those who had the capability to develop such weapons and those motivated to acquire and

use them. Traditionally, terrorist groups interested in acquiring CBRN weapons, such as Aum Shinrikyo and al-Qaeda, have had difficulty recruiting competent scientists with the right expertise and access to the requisite facilities and materials to develop weapons capable of causing mass casualties.[20] By enabling the global, anonymous sale of CBRN-related materials, the Dark Web provides amateur chemists, do-it-yourself (DIY) biologists, and rogue scientists with a means of monetizing their skills without having to run the risks associated with working with an organized criminal group as a middleman or finding their own customers.

Likewise, terrorist groups are no longer limited to recruiting scientists who share their ideology—they can now outsource technical work they are not capable of performing themselves to subject matter experts. Due to the global reach of the Dark Web and the relative ease of shipping chemical, biological, and properly packaged radiological materials without detection, prospective sellers and would-be buyers are not constrained by geography, either.

The use of the Dark Web to acquire CBRN materials is not a hypothetical scenario. In 2013 and 2014, a Florida teenager prepared and sold the toxins abrin and ricin (which is classified as a Schedule 1 chemical weapon under the Chemical Weapons Convention) to customers around the world.[21] Around the same time, another amateur poison aficionado advertised "the production, testing, and sale of biological toxins" on the Dark Web and found buyers for abrin and cyanide in California and New York. Both of these purveyors of poison advertised their wares on a Dark Web marketplace called Black Market Reloaded.[22] While these individuals are now behind bars and Black Market Reloaded has gone offline, these cases illustrate the potential for the Dark Web to be exploited by terrorist groups seeking a shortcut to acquiring CBRN materials or weapons.

Malware

Cyberspace presents another CBRN-related threat: malware. There is a growing risk that non-state actors could use malicious software, or malware, to launch a cyberattack on a facility that produces or stores chemical, biological, radiological, or nuclear materials.

These facilities are increasingly vulnerable to such attacks due to the widespread use of digital and automated industrial control systems and the connection of such systems to computer networks and the internet. As of 2014, there were 2 million industrial control systems connected to the internet—a number that has surely increased since then.[23] In 2014, the Department of Homeland Security was notified of 245 breaches of cybersecurity systems associated with critical infrastructure in the United States, 10 percent of which were part of the nuclear or chemical industries.[24] That same year, the industrial control system at a German iron plant was compromised by an unknown perpetrator, resulting in

"massive damage" to the facility.[25] TRITON, a new type of malware that was specifically designed to compromise the safety systems used in large industrial facilities, emerged in 2017.[26] Several strains of ransomware, a type of malware used to hold infected computer systems hostage until the hackers are paid, that are specifically designed to target industrial control systems have been identified over the last two years.[27] The capability of non-state actors to use sophisticated malware capable of conducting such attacks is growing, based in part on the reverse-engineering of advanced cyberweapons developed by states that have become public.[28]

Facilities containing chemical, biological, radiological, or nuclear materials could be targeted by criminals looking to steal data in order to sell it to the highest bidder or conduct a ransomware attack, by hacktivists opposed to the nuclear or chemical industries, or by terrorists seeking to cause death or destruction. There have already been several incidents around the world where malware has infected nuclear facilities intentionally or unintentionally. Thankfully, none of these infections resulted in the release of radiation.[29] There is a global lack of preparedness for this threat, however. In 2018, the Nuclear Threat Initiative (NTI) found that one-third of countries with weapons-usable nuclear materials or nuclear facilities lacked any of the basic cybersecurity regulations, while two-thirds of such countries do not have plans for responding to a cyberattack on a nuclear facility.[30]

There have already been several incidents where malware has infected nuclear facilities.

Synthetic Biology

Advances in biotechnology, most notably in synthetic biology, also offer new capabilities that could be misused to cause harm. Synthetic biology is a broad term that encompasses tools and capabilities designed to engineer biological systems. One of the most important such capabilities is the ability to synthesize DNA, which allows scientists to create customized genes and even entire viral genomes from scratch.[31] Synthetic biology has emerged as a cornerstone of the growing bioeconomy and a vibrant, global DNA synthesis industry has emerged to satisfy the needs of the biomedical research community as well as the biotech and pharmaceutical industries. The market for goods and services related to synthetic biology is expected to reach US$15 billion by 2025.[32]

In 2015, a scientific advisory panel warned the World Health Organization (WHO) that, based on existing technologies, the barriers to resurrecting the

variola virus that causes smallpox, which had been eradicated from nature and exists in only two secure repositories in the United States and Russia, had fallen so low that the virus could be synthesized "by a skilled laboratory technician or undergraduate students working with viruses in a relatively simple laboratory."[33] The advisory group described the deliberate release of synthesized smallpox virus as a "nightmare scenario" for global health security.[34]

Two years after this dire warning, a Canadian scientist working for an American biotech company and using DNA purchased from a German company brought the world one major step closer to this future by synthesizing horsepox virus, an extinct virus closely related to variola virus.[35] As that scientist told the WHO, the synthesis of horsepox virus "was a stark demonstration that this could also be done with variola virus." Furthermore, "recreation of such viral genomes did not require exceptional biochemical knowledge or skills, significant funds or significant time."[36] That same scientist and company subsequently synthesized vaccinia virus, another virus closely related to variola virus, confirming that their technique is generally applicable to this entire family of pox viruses.[37]

In 2018, the National Academies of Science, Engineering, and Medicine conducted a comprehensive review of the risks posed by emerging biotechnologies and concluded that recreation of known pathogenic viruses was one of the greatest such risks.[38] According to a 2019 global survey of biosecurity practices, no country requires the companies that sell synthetic DNA to prevent "questionable parties" from acquiring materials. The think tank also found that less than 5 percent of countries regulate dual-use research, such as the use of techniques that might also be used to synthesize dangerous viruses.[39] A group of leading DNA synthesis providers, the International Gene Synthesis Consortium (IGSC), has agreed to common standards for screening customers and orders to prevent misuse of their products.[40] This consortium, however, comprises only 80 percent of the DNA synthesis market, leaving many companies operating without biosecurity protocols.

3D Printing

3D printing, also called additive manufacturing, is used to build physical objects layer-by-layer from scratch, in shapes and to standards that are impossible with traditional methods. The major ingredients are a digital build file that contains a 3D blueprint of the object to be built, the raw materials needed to build the object, and a 3D printer. While 3D printers sold for personal use can usually only print in plastic, more advanced machines can print in metal, ceramics, and even biological tissue.

This technology is already being used in the nuclear and aerospace industries, which is significant because both industries demand high-quality, high-strength

parts.[41] Compared to traditional methods, additive manufacturing takes less effort, produces better products, can be done at a fraction of the cost, and requires much less skill due to the automated process. The global additive manufacturing market is expected to grow to over US$34 billion by 2024.[42]

3D printing could be misused to benefit violent non-state actors in several ways. First, 3D printers create new opportunities for DIY proliferation: if a non-state actor is unable to buy or steal a controlled item, they could make it themselves.[43] It is already possible to 3D print drones, handguns, and microreactors that can synthesize chemicals.[44] Second, it is possible for a group using open source software to spread out across different countries to collaborate on a digital design file that any one of them can then use to print the object.[45] And once that digital design file has been created, it can be shared easily and widely via email and the internet in the same way that jihadist groups share ideological materials and bomb-making recipes. Third, a state could covertly assist a terrorist group to acquire a CBRN weapon or delivery system by providing them with a 3D printing capability and the digital design files needed to build some of the key components required for these weapons while not directly transferring any internationally controlled materials or equipment to the group.

While the technology underlying additive manufacturing is advancing rapidly, non-state actors are still a long way from being able to use a 3D printer to build a CBRN weapon.[46] Creating a digital design file of a controlled dual-use item requires extensive knowledge of that item to begin with or a copy of the item that can be scanned to create a digital build file. Advanced 3D printers can cost upward of US$1 million, and operating and maintaining these high-end 3D printers requires some expertise. The most important parts of CBRN weapons, such as fissile materials and pathogens, cannot yet be printed.

The Seven Deadly Traits of Emerging Technologies

These five emerging technologies share seven characteristics that present significant challenges to preventing their misuse.

Dual-Use

First, all of these technological advancements are dual-use: they can be used for peaceful or harmful purposes, making it difficult to control who has access to them and the knowledge and skills necessary to use (or misuse) them. For example, drones developed for recreational purposes and to provide airborne imagery have already been turned into flying IEDs by a few terrorist groups.

Disruptive

Second, these versatile technologies are powerful enough to transform entire industries and fields of science, which makes them highly sought after by individuals, groups, governments, and corporations. All of these technologies were developed initially in academia or the private sector, and their development is being pursued aggressively due to their commercial potential. For example, it has been estimated that products based on engineered biological systems accounted for US$388 billion in revenue in 2017, representing 3 percent of US gross domestic product.[47] The growing bioecomony has been fueled by venture capital; in 2018, synthetic biology companies had their most successful year of attracting private investment, with a combined total of almost US$2 billion in funding across the industry.[48]

Digital

Third, all of these technologies rely to some degree on a digital component, which makes them much easier to share and greatly complicates efforts to regulate them. The build files for 3D printers, the worms and viruses used as cyberweapons, and the genetic sequences used to construct synthetic viruses are completely digital. Before authorities could close a website that hosted the digital build file for a 3D-printed gun, for example, the file was downloaded 100,000 times in just two days.[49] These files have subsequently shown up on websites that cater to DIY 3D printing enthusiasts as well as on the Dark Web.[50]

These technologies rely on a digital component, complicating efforts to regulate them.

Diffused

Fourth, thanks to globalization, these new technologies can now diffuse farther and faster than ever before. The Cambridge, Massachusetts-based nonprofit Addgene, for example, has distributed over 1 million plasmids used in genome editing experiments to over 6,000 laboratories located in more than 100 countries.[51] The purveyors of poison operating on the Dark Web mentioned earlier were able to deliver toxins to customers in Austria, Canada, Denmark, England, and India through the international mail system.[52] The WannaCry ransomware program spread to so many computers so quickly—affecting over 100,000 organizations in more than 150 countries in less than a week in May 2017—by exploiting unpatched vulnerabilities in the file-sharing protocols within and between networks.[53]

Decentralized

Fifth, the global distribution of scientific innovation and industrial capacity has become decentralized: these capabilities are no longer concentrated in advanced economies but are more widely distributed to a more diverse group of nations. For example, the most popular drone models used by terrorist groups in the Middle East are manufactured by the company DIJ based in Shenzhen, China.[54] China's strong investment in biotechnology has also enabled it to become a major player in the field of genome editing.[55] And developing countries are closing the gap in scientific and technological innovation compared to high-income countries.[56] For example, the International Genetically Engineered Machine (iGEM) student competition in synthetic biology attracts a growing number of high school and university teams from outside of North America and Europe.[57]

These technologies more accessible to more people than ever before.

Deskilled

Sixth, the level of expertise needed to successfully use these technologies has been reduced. This process is called deskilling, which makes these technologies more accessible to more people than ever before. More advanced avionics and intuitive flight controls make drones easy to fly, for example, and the highly automated nature of 3D printing reduces the level of skill required to manufacture advanced parts.

Do-It-Yourself

Finally, the convergence of many of these trends has led to the emergence of transnational DIY movements comprising networks of amateur innovators who use open source platforms to build virtual communities dedicated to the development and application of new technologies. The DIY biology movement boasts dozens of community labs and groups in North America, Latin America, Europe, and Asia.[58] DIY Drones, the world's largest group of amateur drone builders and operators, has over 80,000 members around the world.[59] While these groups are overwhelmingly dedicated to the responsible use of these emerging technologies, they tend to operate outside of traditional safety and security regulations. The dynamic nature of these groups and their open membership policies make them difficult to self-police or for law enforcement or intelligence agencies to monitor. These factors raise concerns that these groups might become the unwitting source of knowledge, technology, or expertise that could be used for malicious purposes.

Cautions and Caveats

It is important to note that scientific advances and the emergence of new technologies are not the only, or even the most important, factors influencing the likelihood of terrorist groups acquiring and using CBRN weapons. Thankfully, the number of terrorist groups motivated to acquire these weapons has been limited, despite many that have the requisite technical and financial resources.[60] The vast majority of terrorist groups have been satisfied with conventional weapons such as guns and bombs. The surprising rise of the Islamic State and their repeated use of chemical weapons in Iraq and Syria, however, serve as a reminder that it only takes one group with the intent and capability to acquire and use CBRN weapons to pose a threat to international security.[61]

In addition, the ability of a terrorist group to convert CBRN-related material into a weapon depends on intangible factors such as tacit knowledge (the unarticulated knowledge that can only be gained through hands-on, trial-and-error experience or mentorship), the ability of the group to create and share such knowledge, and its ability to assemble and successfully manage interdisciplinary teams.[62] Terrorist groups, especially those facing pressure from law enforcement and intelligence agencies, have had difficulties recruiting, retaining, and effectively utilizing individuals with the right combination of scientific, technical, and organizational skills to develop effective CBRN weapons.

Developing a CBRN weapon capable of causing mass casualties is also a very complex process. A scientific breakthrough that makes developing or acquiring one component of a weapon easier might not have any impact on the other stages in the weaponization process. Thus, the impact of a single scientific breakthrough or a novel technology on the acquisition of a CBRN weapon should not be exaggerated. For example, synthetic biology might make it easier for a non-state actor to *create* a pathogen, but that technology does not help terrorists improve their ability to *disseminate* the pathogen on a large scale.[63]

Likewise, it is important to assess the specific contributions that a particular technology can make to a specific aspect of the CBRN threat in practice, not just in theory. In the case of 3D printing, this manufacturing technology is not appropriate for working with metals that are toxic or radioactive. While microreactors are well-suited to covertly producing small quantities of highly pure chemicals, they are not well-suited to the production of most chemical warfare agents and precursors due to excessive heat generated by their synthesis and by the production of solid byproducts that would clog the microfluidic channels at the heart of this technology.[64]

Finally, advances in science and technology represent not just threats, but also opportunities to make it harder for terrorist groups to acquire CBRN weapons. Unmanned aerial and ground vehicles can be used for border security, CBRN

weapon detection, and bomb disposal. For example, the EU is sponsoring the development of unmanned aerial and ground vehicles to investigate CBRN crime scenes under the ROCSAFE project.[65] Biometrics and radio frequency ID chips can be used to improve physical security measures and inventory control to prevent unauthorized access to CBRN materials. Advances in science and technology are also leading to improved sensors that can be used to detect the production, transportation, and use of CBRN weapons. The development of dedicated laboratories and new techniques to analyze CBRN materials has also contributed to impressive advances in nuclear, biological, and chemical forensics, which are crucial for attribution.[66]

International Responses

Given the high degree of dual-use, diffusion, and decentralization associated with these emerging technologies, preventing non-state actors from acquiring and using them to cause harm will require international cooperation. There are a number of measures that individual countries, the United Nations, and international organizations dedicated to preventing the proliferation of CBRN weapons, including the International Atomic Energy Agency (IAEA), the Organization for the Prohibition of Chemical Weapons (OPCW), and the Implementation Support Unit (ISU) of the Biological Weapons Convention (BWC), could take to more effectively address this challenge.

One of the international community's most important tools is UNSC Resolution 1540.

One of the international community's most important tools for preventing non-state actors from acquiring CBRN weapons is Resolution 1540, approved by the UN Security Council in 2004. Resolution 1540 requires member states to strengthen border security, physical protection, domestic controls, and export controls to prevent non-state actors from acquiring these weapons and related materials. The resolution also created a committee to oversee implementation of the resolution and a group of experts to provide advice to the committee.[67]

In December 2016, the Security Council unanimously approved Resolution 2325, which renewed and extended 1540's mandate and called upon states to take into account the risks of non-state actors using "rapid advances in science, technology and international commerce for proliferation purposes."[68] Resolution 2325 also added controlling access to intangible transfers of technology as a new nonproliferation obligation for UN member-states. In order to achieve this

objective, the 1540 Committee can organize workshops and training to help countries integrate intangible technology transfers into their export control regulations and raise awareness among relevant stakeholders. This assistance will be particularly important for states that are not members of the Nuclear Suppliers Group (NSG), Missile Technology Control Regime (MTCR), and Australia Group—the multilateral export control regimes for nuclear, missile, or chemical and biological weapons, respectively—as these regimes already contain such requirements.

Resolution 2325 also recognized the need for the 1540 Committee to continue drawing upon the relevant expertise from industry and the scientific and academic communities. The Committee and Group of Experts could initiate an outreach program to academics and scientists in key fields of emerging technologies to complement the committee's ongoing outreach to industry as part of the Wiesbaden Process. This outreach would have the dual benefits of ensuring that the committee has access to up-to-date information on these technologies and educating scientists about the proliferation and terrorism challenges that the committee is charged with addressing.

The United Nations could also bolster the resources available to the Security Council's Counterterrorism Committee and the UN Office of Counterterrorism to support implementation of Resolution 2341, which calls upon member states to strengthen critical infrastructure protection against terrorist threats.[69] The sabotage of nuclear, biological, and chemical facilities using kinetic or cyber weapons could potentially have consequences on par with the use of a weapon of mass destruction. These UN counterterrorism bodies should coordinate their activities in this sphere with those of the 1540 Committee and relevant international organizations that have the requisite expertise in managing chemical, biological, radiological, and nuclear threats.

Interpol, in conjunction with the 1540 Committee, ISU, OPCW, and IAEA, could also help countries establish national mechanisms for bringing together law enforcement authorities and the scientific community. The purpose of such a mechanism would be to create trusted channels of communication between these communities so that if scientists see something suspicious, they know who to contact. The US Federal Bureau of Investigation (FBI)'s WMD Coordinator program, which assigns an agent in every FBI field office to serve as a liaison with local universities and companies that have CBRN-related expertise or materials, provides a useful model.[70]

There also need to be more systematic international reviews of science and technology related to CBRN weapons. The OPCW's Scientific Advisory Board (SAB), which regularly and systematically reviews how advances in chemistry and related fields impact the implementation of the treaty, could serve as a role model.[71] Despite breakthroughs in the life sciences and the global diffusion of

biotechnology, there is no permanent mechanism under the BWC to review how these developments affect the treaty. Instead, reviews of science and technology are undertaken on an *ad hoc* basis by member states and scientific organizations. While these reviews can be high-quality, they are conducted episodically, their scope is limited and determined by national priorities, and discussion of the results receive limited attention during meetings of states parties.[72] While the IAEA reviews developments in science and technology with regard to potential applications for the agency's safeguards mission, the agency does not conduct regular or comprehensive reviews of how emerging technologies might create threats or opportunities related to the security of nuclear materials and facilities.[73]

Finally, Interpol, the OPCW, IAEA, ISU, 1540 Committee, and other relevant international organizations should seek opportunities to harness technology and innovation to enforce Resolution 1540 and support the non-proliferation and disarmament missions of these organizations. Companies and governments are already applying emerging technologies to enhancing export controls, the security of CBRN materials, and forensics, but they may not be attuned to the special needs and considerations of employing these technologies in an international context. In addition, these international organizations typically do not have a research and development budget that would enable them to fund projects that would support their mission. For example, the OPCW has identified a number of technologies that would support its investigative and verification missions, but it does not have the resources to sponsor or develop this technology itself.[74] These international organizations would benefit from having dedicated funding that would enable them to conduct or commission relevant research applicable to preventing non-state actors from acquiring or using CBRN materials as weapons.

The Dark Side of the Fourth Industrial Revolution

The Fourth Industrial Revolution has great potential to improve global prosperity and quality of life. At the same time, the development of technologies driving these profound changes in society and the economy needs to be safeguarded against misuse. Diffusion and decentralization mean that these dual-use technologies are increasingly available on a global basis and therefore require international cooperation to prevent their misuse. The international community needs to take a more active approach to managing the challenge of encouraging innovation and maximizing the benefits of new technologies while attempting to mitigate the risks. A failure to address this challenge proactively will likely lead to unnecessary or counterproductive responses if a non-state actor successfully leverages one of these emerging technologies to conduct a mass casualty attack.

Notes

1. Heather Stewart, "A Terrorist Dirty Bomb? US Summit Asks World Leaders to Plot Response," *Guardian*, April 1, 2016, http://www.theguardian.com/uknews/2016/apr/01/aterroristdirtybombussummitasksworldleaderstoplotresponse.
2. Declan Butler, "Tomorrow's World," *Nature* 530 (February 5, 2016): 398–401, https://doi.org/10.1038/530398a.
3. Klaus Schwab, "The Fourth Industrial Revolution: What It Means and How to Respond," *Foreign Affairs*, December 12, 2015, https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.
4. Schwab, "The Fourth Industrial Revolution."
5. Teal Group, *2016 World Civil UAS Market Profile and Forecast* (Fairfax, VA: Teal Group, 2016), https://www.tealgroup.com/index.php/pages/press-releases/32-teal-group-predicts-worldwide-civil-uas-production-will-total-65-billion-in-its-2016-uas-market-profile-and-forecast.
6. Chris Andersen, "How I Accidentally Kickstarted the Domestic Drone Boom," *Wired*, June 22, 2012, https://www.wired.com/2012/06/ff_drones/.
7. Larry Friese, N.R. Jenzen-Jones, and Michael Smallwood, *Emerging Unmanned Threats: The Use of Commercially-Available UAVs by Armed Non-State Actors*, Special Report No. 2 (Perth, Australia: Armament Research Services, 2016), https://www.academia.edu/37605935/Emerging_Unmanned_Threats_The_use_of_commercially-available_UAVs_by_armed_non-state_actors.
8. Maïa de la Baume, "Unidentified Drones Are Seen above French Nuclear Plants," *New York Times*, November 3, 2014, https://www.nytimes.com/2014/11/04/world/europe/unidentified-drones-are-spotted-above-french-nuclear-plants.html; Hal Bernton, "Who Flew Drone over Bangor Submarine Base? Navy Wants to Know," *Seattle Times*, February 25, 2016, https://www.seattletimes.com/seattle-news/crime/whos-flying-drones-over-bangor-submarine-base-navy-wants-to-know/.
9. Don Rassler, *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology* (West Point, NY: Countering Terrorism Center, October 20, 2016), https://ctc.usma.edu/remotely-piloted-innovation-terrorism-drones-and-supportive-technology/; Don Rassler, *The Islamic State and Drones: Supply, Scale and Future Threats* (West Point, NY: Countering Terrorism Center, July 11, 2018), https://ctc.usma.edu/islamic-state-drones-supply-scale-future-threats/; Anna Ahronheim, "Drones Give Militants New Precision Weapon in Gaza Conflict," *Jerusalem Post*, September 8, 2019, https://www.jpost.com/Middle-East/Drones-Give-Militants-New-Precision-Weapon-In-Gaza-Conflict-601029.
10. Conflict Armament Research, *Iranian Technology Transfers to Yemen* (London: Conflict Armament Research, 2017), https://www.conflictarm.com/download-file/?report_id=2465&file_id=2467; Conflict Armament Research, *Evolution of UAVs Employed by Houthi Forces in Yemen* (London: Conflict Armament Research, 2020), https://www.conflictarm.com/download-file/?report_id=3185&file_id=3189.
11. Nick Waters, "The Poor Man's Air Force? Rebel Drones Attack Russia's Airbase in Syria," *Bellingcat*, January 12, 2018, https://www.bellingcat.com/news/mena/2018/01/12/the_poor_mans_airforce/; Kelsey D. Atherton, "Attacks on an Airbase in Syria Reveal the Cheap Price of Aerial Insurgency," C4SIRnet.com, August 15, 2018, https://www.c4isrnet.com/unmanned/2018/08/15/attacks-on-an-airbase-in-syria-reveal-the-cheap-price-of-aerial-insurgency/.

12. Colum Lynch, "U.N. Questions Evidence against Iran over Missiles," *Foreign Policy*, December 20, 2019, https://foreignpolicy.com/2019/12/20/un-questions-evidence-iran-missiles/; Humeyra Pamuk, "U.S. Probe of Saudi Oil Attack Shows It Came from North – Report," *Reuters*, December 19, 2019, https://www.reuters.com/article/us-saudi-aramco-attacks-iran-exclusive-idUSKBN1YN299.
13. Dennis M. Gormley, "Globalization and WMD Proliferation Networks: The Case of Unmanned Air Vehicles as Terrorist Weapons," *Strategic Insights* 5, no. 6 (July 2006), http://edocs.nps.edu/npspubs/institutional/newsletters/strategic%20insight/2006/gormleyJul06.pdf.
14. Chris Baraniuk, "The Crop-Spraying Drones That Go Where Tractors Can't," *BBC News*, August 3, 2018, https://www.bbc.co.uk/news/business-45020853.
15. Anthony T. Tu, "Overview of Sarin Terrorist Attacks in Japan," *ACS Symposium Series* 745 (2000): 304–17, https://doi.org/10.1021/bk-2000-0745.ch020.
16. Shusuke Murai, "Man Who Landed Drone on Roof of Japanese Prime Minister's Office Gets Suspended Sentence," *Japan Times*, February 16, 2016, https://www.japantimes.co.jp/news/2016/02/16/national/crime-legal/man-landed-drone-roof-japanese-prime-ministers-office-gets-suspended-sentence/#.Wxq8I4pKiUk.
17. Daniel Moore & Thomas Rid, "Cryptopolitik and the Darknet," *Survival* 58, no. 1 (2016): 7–38, https://doi.org/10.1080/00396338.2016.1142085; Giacomo Persi Paoli et al., *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (Cambridge, UK: RAND Europe, 2017), https://doi.org/10.7249/RR2091.
18. Robleh Ali et al., "Innovations in Payment Technologies and the Emergence of Digital Currencies," *Bank of England Quarterly Bulletin* 54, no. 3, (2014): 262–75, https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/quarterly-bulletin-2014-q3.pdf; Robleh Ali et al., "The Economics of Digital Currencies," *Bank of England Quarterly Bulletin* 54, no. 3 (2014): 276–86, https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/quarterly-bulletin-2014-q3.pdf.
19. Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* (Paris: FATF, June 2014), https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf; Iwa Salami, "Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?" *Studies in Conflict and Terrorism* 41, no. 12 (2018), https://doi.org/10.1080/1057610X.2017.1365464.
20. Anne Stenersen, *Al Qaida's Quest for Weapons of Mass Destruction: The History Behind the Hype* (Saarbrucken, Germany: VDM Verlag Dr. Muller, 2008); Richard Danzig et al., *Aum Shinrikyo: Insights into How Terrorists Develop Biological and Chemical Weapons* (Washington, DC: Center for New American Security, 2012), https://s3.amazonaws.com/files.cnas.org/documents/CNAS_AumShinrikyo_SecondEdition_English.pdf.
21. US Attorney's Office District of New Jersey, "Florida Man Admits Role in International Murder Conspiracy and Sale and Smuggling of Deadly Toxins," FBI.gov, August 12, 2014, https://www.fbi.gov/contact-us/field-offices/newark/news/press-releases/florida-man-admits-role-in-international-murder-conspiracy-and-sale-and-smuggling-of-deadly-toxins.
22. US Department of Justice, "Florida Man Sentenced to 110 Months in Prison for Conspiring to Murder a Foreign National and for Sale and Smuggling of Deadly Toxins," FBI.gov, February 18, 2015, https://www.fbi.gov/contact-us/field-offices/newark/news/press-releases/florida-man-sentenced-to-110-months-in-prison-for-conspiring-to-murder-a-foreign-national-and-for-sale-and-smuggling-of-deadly-toxins; Sam Stanton and Denny Walsh,

"Federal Court Documents Link Carmichael Man to S.F. Bomb, Toxin Case," *Sacramento Bee*, June 8, 2014, https://www.sacbee.com/news/local/crime/article2600824.html.
23. Infracritical, *Project SHINE (SHodan INtelligence Extraction) Findings Report*, October 1, 2014, https://www.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014.
24. Department of Homeland Security, *ICS-CERT Monitor*, September 2014–February 2015, 1–3, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf
25. Rachael King, "Cyberattack on German Iron Plant Causes 'Widespread Damage': Report," *Wall Street Journal*, December 18, 2014, https://blogs.wsj.com/cio/2014/12/18/cyberattack-on-german-iron-plant-causes-widespread-damage-report/.
26. Andy Greenberg, "A Look into the Toolkit of the Dangerous Triton Hackers," *Wired*, April 10, 2019, https://www.wired.com/story/triton-hacker-toolkit-fireeye/.
27. Andy Greenberg, "Mysterious New Ransomware Targets Industrial Control Systems," *Wired*, February 3, 2020, https://www.wired.com/story/ekans-ransomware-industrial-control-systems/; Dragos, "Malware Infections Increase at Industrial Companies Globally," April 20, 2020, https://dragos.com/blog/industry-news/malware-infections-increase-at-industrial-companies-globally/.
28. Lily Hay Newman, "The Leaked NSA Spy Tool that Hacked the World," *Wired*, March 7, 2018, https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/; Gil Baram, "The Theft and Reuse of Advanced Offensive Cyber Weapons Pose A Growing Threat," Net Politics (blog), Council on Foreign Relations, June 19, 2018, https://www.cfr.org/blog/theft-and-reuse-advanced-offensive-cyber-weapons-pose-growing-threat.
29. Caroline Baylon, Roger Brunt, and David Livingstone, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks* (London: Chatham House, 2015), https://www.chathamhouse.org/sites/default/files/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf.
30. Nuclear Threat Initiative, *Nuclear Security Index: Building a Framework for Assurance, Accountability, and Action*, 4th ed. (Washington, DC: Nuclear Threat Initiative, 2018), 15–17, https://ntiindex.org/wp-content/uploads/2018/08/NTI_2018-Index_FINAL.pdf.
31. Narayana Annaluru, Sivaprakash Ramalingam, and Srinivasan Chandrasegaran, "Rewriting the Blueprint of Life by Synthetic Genomics and Genome Engineering," *Genome Biology* 16 (2015): 125–37, https://doi.org/10.1186/s13059-015-0689-y.
32. Market Research Engine, *Synthetic Biology Market - Global Industry Analysis and Forecast 2020-2025*, January 2020, https://www.marketresearchengine.com/reportdetails/synthetic-biology-market.
33. *The Independent Advisory Group on Public Health Implications of Synthetic Biology Technology Related to Smallpox* (Geneva: World Health Organization, June 2015), 18, http://apps.who.int/iris/bitstream/10665/198357/1/WHO_HSE_PED_2015.1_eng.pdf.
34. *The Independent Advisory Group*, 11.
35. Gregory D. Koblentz, "The De Novo Synthesis of Horsepox Virus: Implications for Biosecurity and Recommendations for Preventing the Reemergence of Smallpox," *Health Security* 15, no. 6 (August 2017): 1–9, https://doi.org/10.1089/hs.2017.0061.
36. WHO Advisory Committee on Variola Virus Research, *Report of the Eighteenth Meeting* (Geneva: WHO, May 2017), 29, https://www.who.int/csr/resources/publications/smallpox/18-ACVVR-Final.pdf.

37. Gregory D. Koblentz, "A Biotech Firm Made a Smallpox-Like Virus on Purpose. Nobody Seems to Care," *Bulletin of the Atomic Scientists*, February 21, 2020, https://thebulletin.org/2020/02/a-biotech-firm-made-a-smallpox-like-virus-on-purpose-nobody-seems-to-care/
38. National Academies of Science, Engineering, and Medicine, *Biodefense in the Age of Synthetic Biology* (Washington, DC: National Academies Press, 2018), 38–42, 117–18, https://www.nap.edu/catalog/24890/biodefense-in-the-age-of-synthetic-biology.
39. Nuclear Threat Initiative, *Global Health Security Index* (Washington, DC: Nuclear Threat Initiative, October 2019), https://www.ghsindex.org/wp-content/uploads/2019/10/2019-Global-Health-Security-Index.pdf
40. Koblentz, "The De Novo Synthesis of Horsepox Virus."
41. Grant Christopher, "3D Printing: A Challenge to Nuclear Export Controls," *Strategic Trade Review* 1, no. 1 (Autumn 2015): 18–25, https://strategictraderesearch.org/wp-content/uploads/2017/11/STR_01.pdf.
42. *3D Printing Market Global Forecast to 2024* (Northbrook, IL: Markets and Markets, October 2019), https://www.marketsandmarkets.com/Market-Reports/3d-printing-market-1276.html.
43. Matthew Kroenig and Tristan Volpe, "3-D Printing the Bomb? The Nuclear Nonproliferation Challenge," *Washington Quarterly* 38, no. 3 (Fall 2015): 7–19, https://doi.org/10.1080/0163660X.2015.1099022; Kolja Brockmann, "Advances in 3D Printing Technology: Increasing Biological Weapon Proliferation Risks?" WritePeace (blog), Stockholm International Peace Research Institute, July 29, 2019, https://www.sipri.org/commentary/blog/2019/advances-3d-printing-technology-increasing-biological-weapon-proliferation-risks.
44. Benjamin King and Glenn McDonald, eds., *Behind the Curve: New Technologies, New Control Challenges* (Geneva: Small Arms Survey, Graduate Institute of International and Development Studies, 2015), http://www.smallarmssurvey.org/fileadmin/docs/B-Occasional-papers/SAS-OP32-Behind-the-Curve.pdf; Emma Sargent, "3D-Printed Miniaturised Fluidic Devices," Chemistry World, August 8, 2012, https://www.chemistryworld.com/news/3d-printed-miniaturised-fluidic-devices-/5317.article; Tiaan Roux, "Are 3D printed UAVs Really the Future?" *sUAS News*, January 2, 2017, https://www.suasnews.com/2017/01/3d-printed-uavs-really-future/.
45. Matthew Hallex, "Digital Manufacturing and Missile Proliferation," *Public Interest Report* 66, no. 2 (Spring 2013), https://fas.org/pir-pubs/digital-manufacturing-and-missile-proliferation/.
46. Christopher, "3D Printing"; Amy Nelson, "The Truth about 3-D Printing and Nuclear Proliferation," *War on the Rocks*, December 14, 2015, http://warontherocks.com/2015/12/the-truth-about-3-d-printing-and-nuclear-proliferation/.
47. *Engineering Our Way to a Sustainable Bioeconomy: Hearing before the House Subcommittee on Research and Development of the House Committee on Space, Science, and Technology*, 116th Cong. (March 12, 2019) (testimony of Robert Carlson), https://docs.house.gov/meetings/SY/SY15/20190312/109051/HHRG-116-SY15-Wstate-CarlsonR-20190312.pdf.
48. John Cumbers et al., *Synthetic Biology Annual Investment Report* (Pleasant Hill, CA: SynbioBeta, 2018), https://synbiobeta.com/reports/investment-report-2018/.
49. Andy Greenberg, "3D-Printed Gun's Blueprints Downloaded 100,000 Times in Two Days (with Some Help from Kim Dotcom)," *Forbes*, May 8, 2013, https://www.forbes.com/sites/andygreenberg/2013/05/08/3d-printed-guns-blueprints-downloaded-100000-times-in-two-days-with-some-help-from-kim-dotcom/#19323af310b8.

50. Brittany Sevenson, "Free for All! Liberator 3D Printable Gun Files Are Currently Being Downloaded on Thingiverse," *3DPrint.com*, May 13, 2015, https://3dprint.com/65142/free-for-all-liberator-3d-printable-gun-files-are-currnetly-being-downloaded-on-thingiverse/; Whitney Hippolite, "3D Printable Files for Cody Wilson's Liberator Gun are Now Available to All on 3DShare," *3DPrint.com*, June 18, 2015, https://3dprint.com/73842/download-3d-printed-gun/; Giacomo Persi Paoli et al., *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (Santa Monica, CA: RAND, 2017), 34, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2091/RAND_RR2091.pdf.
51. Caroline M. LaManna and Rodolphe Barrangou, "Enabling the Rise of a CRISPR World," *CRISPR Journal* 1, no. 3 (2018): 205, https://doi.org/10.1089/crispr.2018.0022.
52. US Attorney's Office, "Florida Man Admits Role."
53. "Timeline: How the WannaCry Cyber Attack Spread," *Financial Times*, May 14, 2017, https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23.
54. Dan Gettinger, *Drones Operating in Syria and Iraq* (Bard College: Center for the Study of Drones, 2016), https://dronecenter.bard.edu/files/2016/12/Drones-in-Iraq-and-Syria-CSD.pdf.
55. Jon Cohen and Nirja Desai, "With Its CRISPR Revolution, China Becomes a World Leader in Genome Editing," *Science*, August 2, 2019, https://www.sciencemag.org/news/2019/08/its-crispr-revolution-china-becomes-world-leader-genome-editing.
56. Soumitra Dutta, Bruno Lanvin, and Sacha Wunsch-Vincent, eds, *The Global Innovation Index 2017: Innovation Feeding the World* (Geneva: World Intellectual Property Organization, 2017), http://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2017.pdf.
57. "Teams Information," iGEM, 2017, http://2017.igem.org/Teams.
58. DIYbiosphere (website), accessed 2020, http://sphere.diybio.org/.
59. DIY Drones: The Leading Community for Personal UAVs (website), accessed 2020, https://diydrones.com/.
60. Jonathan B. Tucker, ed., *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons* (Cambridge: MIT Press, 1999).
61. Columb Strack, "The Evolution of the Islamic State's Chemical Weapons Efforts," *CTC Sentinel* 10, no. 9 (October 2017): 19–23, https://ctc.usma.edu/the-evolution-of-the-islamic-states-chemical-weapons-efforts/.
62. Kathleen M. Vogel, *Phantom Menace or Looming Danger?: A New Framework for Assessing Bioweapons Threats* (Baltimore, MD: Johns Hopkins University Press, 2012); Sonia Ben Ouagrham-Gormley, *Barriers to Bioweapons: The Challenges of Expertise and Organization for Weapons* (Ithaca, NY: Cornell University Press, 2014).
63. Gerald L. Epstein, "The Challenges of Developing Synthetic Pathogens," *Bulletin of the Atomic Scientists*, May 19, 2008, https://thebulletin.org/2008/05/the-challenges-of-developing-synthetic-pathogens/.
64. Andreas Zaugg, Julien Ducry, and Christophe Curty, "Microreactor Technology in Warfare Agent Chemistry," *Mil. Med. Sci. Lett. (Voj. Zdrav. Listy)* 82, no. 2 (2013): 63–68, https://www.mmsl.cz/pdfs/mms/2013/02/03.pdf.
65. Anthony King, "Sherlock Drones: Automated Investigators Tackle Toxic Crime Scenes," *Horizon* (EU), March 14, 2018, https://horizon-magazine.eu/article/sherlock-drones-automated-investigators-tackle-toxic-crime-scenes_en.html.
66. Joint Working Group of the American Physical Society and the American Association for the Advancement of Science, *Nuclear Forensics: Role, State of the Art, Program Needs* (Washington, DC: AAAS, 2008), https://www.aps.org/policy/reports/popa-reports/

upload/nuclear-forensics.pdf; Bruce Budowle et al., eds., *Microbial Forensics*, 2nd ed. (Amsterdam: Elsevier, 2011); Organization for the Prohibition of Chemical Weapons, *Report of the Scientific Advisory Board's Workshop on Chemical Forensics* (The Hague: OPCW, July 14, 2016), https://www.opcw.org/sites/default/files/documents/SAB/en/sab24wp01_e_.pdf.

67. Daniel Salisbury, Ian J. Stewart, and Andrea Viski, eds., *Preventing the Proliferation of WMDs: Measuring the Success of UN Security Council Resolution 1540* (Cham, Switzerland: Palgrave Pivot, 2018).
68. United Nations Security Council Resolution 2325, December 15, 2016, http://unscr.com/en/resolutions/doc/2325.
69. United Nations Security Council Resolution 2341, February 13, 2017, http://unscr.com/en/resolutions/doc/2341.
70. Kristin Hummel, "A View from the CT Foxhole: Edward You, FBI Weapons of Mass Destruction Directorate, Biological Countermeasures Unit," *CTC Sentinel* 10, no. 7 (August 2017): 9–12, https://ctc.usma.edu/a-view-from-the-ct-foxhole-edward-you-fbi-weapons-of-mass-destruction-directorate-biological-countermeasures-unit/.
71. Organization for the Prohibition of Chemical Weapons, *Report of the Scientific Advisory Board on the Developments in Science and Technology for the Fourth Special Session of the Conference of State Parties to Review the Operation of the Chemical Weapons Convention* (The Hague: OPCW, April 30, 2018), https://www.opcw.org/sites/default/files/documents/CSP/RC-4/en/rc4dg01_e_.pdf
72. Caitriona McLeish and James Revill, *Keeping Up with the Scientists*, BWC Review Conference Paper No. 2 (Oslo, Norway: International Law and Policy Institute, 2016), http://bwc1972.org/wp-content/uploads/2016/10/02-Keeping-up-with-the-scientists-gold.pdf.
73. Interview with Laura S. H. Holgate, former US Ambassador to the International Atomic Energy Agency, June 4, 2019.
74. Organization for the Prohibition of Chemical Weapons, *Summary of the Second Meeting of the Scientific Advisory Board's Temporary Working Group on Investigative Science and Technology* (The Hague: OPCW, January 21, 2019), https://www.opcw.org/sites/default/files/documents/2019/01/sab28wp02%28e%29.pdf