The Technologies and International Politics of Genetic Warfare

Yelena Biberman

Abstract

This article considers the prospect and potential of genetic warfare. Drawing on expert interviews and fieldwork, it begins by detailing how the recent and anticipated innovations in synthetic biology, artificial intelligence, and nanotechnology solve the weaponization, delivery, and precision problems that had previously made biological weapons impractical. The article then considers how states and non-state actors may develop and use genetic weapons, with a focus on the problem of secrecy. Underlying whether to reveal or conceal genetic war capability is a trade-off between strategic surprise and deterrence. Actors requiring deterrence are likely to reveal genetic military capability. With the only rivaling source of deterrence being nuclear weapons, nonnuclear states and non-state actors are more likely to make public their genetic weapons capability than nuclear states. The question of whether to use genetic weapons covertly or openly also entails a trade-off. Covert use confers strategic and tactical benefits, whereas the benefits of unrestricted use are primarily psychological. Terroristic, genocidal, and apocalyptic regimes and non-state actors may use genetic weapons openly, but most would likely opt for covert genetic warfare.

*****

Is the genome becoming a new domain of warfare? Innovations in synthetic biology, artificial intelligence (AI), and nanotechnology are hastening the prospect of human evolution catching up with shifting cultural preferences.[1] The capacity to modify itself by environmental demands may enable the so-called *Homo deus* to survive and thrive despite the many possible impediments.[2] However, the revolutionary technologies may also usher in human extinction.

In making his case for reelection in 2012, Vladimir Putin predicted that nuclear weapons would, over the next half a century, become eclipsed by "fundamentally new instruments for achieving political and strategic goals."[3] The future of warfare, he said, is "based on new physical principles," including "genetic" science. The new weapons would be "as effective as nuclear," but

"more 'acceptable' from the political and military perspective."[4] Then came a construction boom at over two dozen institutes that had previously comprised the USSR's biological and chemical weapons establishment.[5]

The US security establishment is also beginning to take the promises and perils of the biotechnology revolution seriously, and there have been calls for a national strategy.[6] The US intelligence community's (IC) 2016 worldwide threat assessment singled out genome editing: "Research in genome editing conducted by countries with different regulatory or ethical standards than those of Western countries probably increases the risk of the creation of potentially harmful biological agents or products."[7] The IC predicted, however, that researchers will "continue to encounter challenges to achieve the desired outcome of their genome modifications, in part because of the technical limitations that are inherent in available genome editing systems."[8]

The Imperiale Framework—developed by the National Academies of Sciences, Engineering, and Medicine in 2018 at the behest of the US Department of Defense—offers the latest, most complete assessment of the hierarchy of probable biological threats. It begins by noting that the scientific advances of the past two decades have expanded what is possible in creating new weapons while also making them more quickly available and more widely accessible.[9] The Imperiale Framework identifies three capabilities warranting the most concern at present: recreating known pathogenic viruses, making existing bacteria more dangerous, and making harmful biochemicals via in situ synthesis. The first two rely on technology that is easy to use and highly accessible; the novelty of the third makes preventing and recognizing an attack particularly difficult.[10]

This article explores the prospect and potential of genetic weapons, or genetically engineered bioweapons. It begins by surveying the recent technological developments that make genetic weapons possible. These include vital advancements in synthetic biology, AI, bioinformatics, nanotechnology, and robotics. These advancements make genetic weapons potentially at least as dangerous as nuclear but as accessible as cyber weapons.

It then considers how states and non-state actors may develop and use genetic weapons, specifically regarding secrecy. The recent COVID-19 pandemic triggered fears and high-level, questionable accusations of covert biological warfare.[11] The response suggests that even if the worry is unwarranted in the COVID-19 case, questions about the covert capability and use of bioengineered weapons are likely to surface in policy, politics, and popular culture over the decades to come. Regarding genetic weapons capability, this article proposes that the choice to reveal or conceal involves

a trade-off between strategic surprise capability and deterrence. Consequently, actors seeking to deter rivals—be it from an offensive attack or retaliation—would likely reveal genetic military capability. Such is especially the case when these actors do not already possess the only rivaling source of deterrence: nuclear weapons. Nonnuclear states and non-state actors would, therefore, be most likely to make public their genetic weapons capability. The actors most likely to conceal it are nuclear states.

The question of whether to use genetic weapons covertly or openly also entails a trade-off. Covert use confers strategic and tactical benefits, such as tactical surprise, plausible deniability, and versatility. The benefits of unrestricted use are primarily psychological and symbolic.[12] Consequently, those seeking genetic weapons' psychological or symbolic benefits would be most likely to use genetic weapons openly. This category comprises terroristic, genocidal, and apocalyptic regimes and non-state actors.[13] Others would likely opt for covert use.

Technologies of Genetic Warfare

Biological weapons have been dubbed "a failed military innovation."[14] The United States and USSR researched and produced them during the Cold War but did not use them.[15] With a few horrific exceptions, modern states have not turned biological agents into weapons of choice.[16]

Experts widely regard biological weapons as "inefficient, unpredictable, and more likely to harm their users than their intended targets."[17] Effective use requires overcoming three sets of obstacles. The first is that of weaponization or turning a biological agent into a working weapon. Here arise questions of availability, infectivity, casualty effectiveness, immunization, and therapy.[18] That is, is the agent capable of producing an infection that would interfere with the target's normal activities in the desired way and against which the target is defenseless?

The second set of obstacles concerns the agent's delivery. Here arise questions of resistance, epidemicity, and detection. How will the agent reach the target? Can it maintain its virulence outside of the lab by withstanding destructive environmental conditions, such as the ultraviolet radiation of sunlight? Will it mutate? How will it spread from host to host?

Finally, there is the question of precision. Biological weapons have seen minimal modern battle mainly because they are indiscriminate, affecting all exposed to them.[19] Targeting and blowback ("retroactivity") are as critical as those of weaponizability and delivery. Could the biological agent be used selectively against a specific target? Could it backfire against those using it?

Some have been understandably circumspect about the potential of the recent advances in biotechnology to cause serious threats. For example, Sonia Ben Ouagrham-Gormley highlights unpredictability as a significant problem in processing and handling any biomaterials, which "evolve, are prone to developing new properties, and are sensitive to environmental and handling uncertainties."[20] Weapons relying on biomaterials will, she argues, always be "captive to the complexity of living systems, and despite the progress made in understanding their functions and composition, the process of creating and maintaining viable organisms still retains a great deal of mystery."[21] The complexity of living systems can be both a challenge and a potential benefit to keeping organisms viable. The recent experience with the mutating coronavirus has demonstrated what Charles Darwin observed in *Origin of Species* (and Jeff Goldblum reaffirmed in *Jurassic Park*): life finds a way. A virus that can survive contact with the human immune system can better mutate to avoid the immune response. Among the other challenges to progress previously identified in the literature are software development and management of large data sets, and social and economic factors, such as organizational pathologies and market failures.[22] The National Academy of Sciences lists several bottlenecks to synthetic biology-enabled capability, but it also predicts that some of them "will likely widen and some barriers will be overcome."[23] In other words, science finds a way.

The following explains how emerging technologies are enabling state and non-state actors to overcome the traditional impediments to biological warfare. It identifies some of the existing challenges and the breakthroughs that suggest that overcoming these challenges is only a matter of time.

Weaponizability

Biological weapons do not require genetic engineering. However, the new techniques for changing an organism's genetic makeup open the possibility "to develop—either deliberately or accidentally—pathogens with enhanced transmissibility or lethality, including entirely new kinds of biological agents and toxins."[24] Neither engineering existing living organisms nor creating novel ones would be possible, however, without the "super-exponential growth" in genomic data generation over the past decade due to advances in sequencing technologies, bioinformatics, and artificial intelligence.[25]

The global leader in DNA sequencing is China. In 2010, BGI (formerly the Beijing Genomics Institute and now a Shenzen-based firm) purchased 128 of the world's fastest sequencing machines, gaining more than half the

global capacity for decoding DNA.[26] Its stated goal is to sequence the genomes of one million people, one million plants and animals, and one million microbial ecosystems.[27] Other successful sequencing companies include Beijing-based Novogene, founded in 2011 by a former BGI executive.

Genomics research is characterized by a culture of open access sharing of large-scale DNA sequence data, a legacy of the Human Genome Project.[28] The exponentially increasing volume of genomic data is prompting initiatives to make the data more accessible.[29] Even data storage is being pursued genetically. In a study published in 2017, researchers efficiently encoded onto a speck of DNA information such as an entire computer operating system, a film, a $50 Amazon gift card, and a computer virus and then successfully retrieved all the digital content. The process is still costly, but the study revealed that "DNA has the potential to provide large-capacity information storage"—millions of megabytes of information could be stored in a single gram of DNA.[30]

Making the plethora of genomic data legible is AI, which uses computer systems to do what previously required human intelligence.[31] For example, the artificial neurons of a group of algorithms known as "deep learning" make accessible to humans vast and complex data sets.[32] The tools and techniques for the analysis, storage, and distribution of genomic data (i.e., bioinformatics), especially when combined with artificial intelligence, also enable simulation that could be used to optimize genomic weaponization.

In 2015, CRISPR (clustered regularly interspaced short palindromic repeats) ushered a "huge revolution" in gene editing by "effectively democratiz[ing] the technology so that everyone is using it."[33] It is now allowing researchers to cheaply and quickly change the DNA of almost any organism, including human.[34] The CRISPR technique relies on a class of enzymes (called "Cas" for "CRISPR-associated," Cas9 in particular) that uses a guide RNA molecule to pinpoint its target DNA that then edits the DNA to disrupt genes or to insert desired sequences. Researchers typically need to order only the RNA fragment, as the other components can be bought off the shelf. The total cost of gene editing is as little as $30, and the technique is even taught in middle-school science classes.[35] CRISPR's affordability, availability, and ease of use increase the prospects of its misuse "not only by a malicious actor but also through accident."[36]

Technologies such as CRISPR are, as the US intelligence community's 2016 worldwide threat assessment put it, "almost always dual-use" and "diffuse rapidly around the globe."[37] And research is gradually overcoming its technical limitations. In 2015, the first human embryos were genetically engineered using CRISPR.[38] Efficiency was low, some cells were altered

while others were not within the same embryo, and "off-target" mutations were observed. However, in just two years, these problems were largely overcome. Scientists repaired a severe disease-causing mutation by successfully editing genes in human embryos. In the ensuing embryos, all cells were mutation-free, and there was no evidence of off-target mutations.[39]

In 2020, the United States turned to CRISPR to battle the SARS-CoV-2 coronavirus causing the COVID-19 disease. The Food and Drug Administration granted its first "emergency-use" approval for a coronavirus test involving CRISPR, selected for its ability to detect (and signal with fluorescent glow) SARS-CoV-2 genetic material from a nose, mouth, or throat swab in about an hour.[40]

The CRISPR approach is relatively simple and widely accessible, but applying it successfully to accomplish a specific change in an organism is still a work in progress. An analogy is word processing on a computer. It is easy to edit a document but very difficult to generate a novel. The latter still takes unique expertise and experience.[41] It is not easy to obtain, maintain, and successfully propagate living organisms. It is harder still to figure out what DNA to change and how to accomplish a specific change in the function of an organism. The CRISPERed human embryos edited out genetic diseases, but it took decades to identify the exact genetic mutations causing them. They were all relatively simple genetic mutations and disorders. Most biological traits have a more complex genetic basis. Even if a simple pathogen is selected and made more virulent or weaponized, it is still challenging to scale up production and mass produce.

Genetic editing is not the only route to weaponization, however. An infectious agent can be synthesized. Its DNA can be created from scratch using chemical precursors and then inserted into a host cell where it can "come alive."[42] In 2002, a team of researchers from the State University of New York at Stony Brook synthesized an artificial poliovirus from scratch.[43] They obtained the virus's genetic sequence online; ordered small, tailor-made DNA sequences; and combined them to reconstruct the complete viral genome. They then added a chemical cocktail to bring the synthesized DNA to life. Such a method could synthesize other viruses with similarly short DNA sequences, such as Ebola.

The field of synthetic biology, which involves "selectively altering the genes of organisms to make them do things that they would not do in their original, natural, untouched state," is advancing rapidly.[44] It essentially treats biological systems as computers—as "programmable manufacturing systems"—by "making small changes in their genetic software" to "effect big changes in their output."[45] A variety of genetic engineering strategies are

now available to "increase control" over genetic interactions, such as pleiotropy (a single gene having more than one, seemingly unrelated, effect).[46]

Delivery

In 1963, the CIA tried to assassinate Cuban leader Fidel Castro with biological weapons. The unwitting assassin was American lawyer James Donovan (notably played by Tom Hanks in the Oscar-nominated movie *Bridge of Spies*). Donovan was conducting the first-ever secret negotiations with Castro and planning to give him a scuba diving suit as a confidence builder. The CIA planned to contaminate the scuba suit and the accompanying breathing apparatus with Madura foot fungus (causing a chronic skin infection) and tuberculosis bacteria. However, the plot was shelved when an agency insider alerted Donovan to possible CIA tampering.[47]

Arranging for a biological warfare agent to be absorbed through (or injected into) the target's skin is, as the case of Castro shows, a logistical nightmare. Even if such a delivery method may be effectively used for assassination, it is unlikely to be used to cause mass casualties.

Biological warfare agents can be disseminated in several other ways. Aerosol sprays disperse airborne germs as fine particles. However, they require the target to breathe a sufficient quantity of the particles into the lungs. Many toxins lose their toxicity when aerosolized as well as when the aerosol cloud enters the atmosphere. A sudden change in wind direction may also impair the entire operation. On four separate occasions, the Japanese religious cult Aum Shinrikyo ("Supreme Truth"), notorious for its 1995 nerve gas attack, attempted to spray a bacterial agent over Tokyo. Despite its "impressive resources, dedicated personnel, and high motivation," none of the efforts succeeded, illustrating that it is "far more difficult to carry out a deadly bioterrorism attack than has sometimes been portrayed."[48] Aum carried out its attacks during the summer, with sunlight and smog likely degrading the bacterial agent. One of the attacks was during a rainy month, so the aerosolized particles were likely washed out of the air.[49]

Another bioweapons delivery mechanism is explosives, whether artillery, missiles, or detonated bombs. The explosives method is even less effective than aerosols because the blast destroys about 95 percent of the disease-causing agent. Deadly agents can also be put into food or water. The logistics are a significant limiting factor here as well. Contaminating a city's water supplies, for example, requires "an unrealistically large" amount of an agent.[50]

Delivery problems have made biological weapons tactically unappealing.[51] Effective delivery requires the deadly agent to reach its target. Doing so requires a robust agent and a reliable delivery mechanism. New technologies are enabling both.

Most bacterial and viral agents struggle to maintain their virulence when confronted with common environmental factors, such as sunlight and humidity, and high temperatures or radical temperature changes. They also evolve and mutate. Genetic instability is typical for microorganisms. With increased transmissibility often comes reduced virulence. Production of virus molecules involves passage through host organisms. As the virus is not subject to any evolutionary pressure to maintain virulence during this scaling-up process, it tends to accumulate mutations that generate an attenuated strain. Similarly, bacteria cultured in laboratories tend to lose virulence.[52]

Gene editing and synthetic biology research are making strides in overcoming the problem of genetic instability. A study published in 2019 presented a new system, CRISPR-BEST. It created mutations in actinomycetes (bacteria that produce a wide variety of industrially and medically relevant compounds) without creating genetic instability and forcing them to rearrange and even delete large parts of their chromosomes.[53] Synthetic biology is also increasingly embracing genetic instability rather than trying to suppress or compensate for it. With improved understanding, it is expected to design devices that incorporate genetic instability as a parameter.[54] Such devices would be "a true frontier in biological engineering."[55]

When it comes to delivery, nanotechnology can prevail where aerosols, explosives, and in-person methods falter. Nanotechnology exploits the behavior of materials ranging from 1 to 100 nanometers, visible only through the most powerful microscopes.[56] In their suggestions for a new NATO Strategic Concept, a group of experts (led by former US secretary of state Madeleine Albright) identified nanotechnology as a "potentially disruptive development" that could "transform the technological battlefield."[57]

Nanotechnology offers new delivery possibilities for biological and genetic weapons. In the future, nano-carriers and capsules may transport small toxins, such as ricin or microbe subunits (e.g., the lethal factor of anthrax), across otherwise impermeable cell membranes and the blood-brain barrier. Bioagents' targeted delivery with nanoparticles is likely to increase effectiveness and, thus, require less of the agent.[58] Nanotechnology could also enable controlling biological weapons once they enter the body.[59]

Speculative literature predicts the production of nanoscale robots that would enter the body and penetrate cells, causing them to act similarly to

the effects of a biological or chemical weapon.[60] Experts also speculate that, in the future, "insect-like" nanobots could be programmed to inject toxins into humans.[61] No scuba gear required.

The field of synthetic biology encompasses hybrid technology that combines living and nonliving elements.[62] Biological organisms can be enhanced with nanotechnology, or nanotechnology (e.g., nanobots) can be enhanced with biological elements. This includes technology-enhanced organisms (or viruses) at one end of the spectrum and biologically-enhanced machines at the other end. Somewhere in the middle, an organism crosses the line between living and nonliving. The latter would not have the inherent capacity to mutate, reproduce, and evolve.

Combining genetically engineered DNA using CRISPR and nanotechnology-based vectors for packaging and delivery could help overcome the inherent liabilities of natural biological weapons. It would make them more durable, efficient, and precise. Since they would not be alive and would not evolve, their behavior would be much more predictable and amenable to engineering than living agents would be. Synthetic biology could be used to create "smart germs" that combine the biological functions of DNA with synthetic manufacturing, delivery, and targeting systems that include hybrid biological and synthetic mechanisms. An example might be a nanoscale microchip that is ingested or breathed in, activated by a specific host, that uses a microfluidic chip and engineered DNA to absorb reagents from the host's body and manufacture a specific toxin or pathogen.

Precision

Could a weaponized biological agent be delivered to the intended target and affect only that target? This is the problem of precision, and, like the problems of weaponizability and delivery, it had made biological weapons unreliable. New technologies allow precise or selective targeting by tailoring deadly agents specifically for a given group or individual.

The idea of using genetic information to target specific groups with biological or chemical weapons was first publicly aired in 1970 in *Military Review*, the US Army's professional journal. The article considers the prospect of weaponizing genetic differences—specifically in the activities of enzymes—between different ethnic groups. That is, certain groups may be more vulnerable than others to a given naturally occurring agent.[63] Written before the age of genetic engineering and biotechnology, the article drastically underestimates what is possible.

There are far more genetic similarities between individuals and human populations than differences. However, differences exist. This is not because social categories like ethnicity or race are biological but because populations differ in the frequencies of some alleles (i.e., marker alleles) they carry. The differences are a product of microevolution as the human species spread around the globe and adapted to living in different environments.[64] A case in point is the adaptation to malaria through a high frequency of sickle cell anemia found in populations in West Africa.[65]

Over time, natural selection spreads across human populations' genetic variants, granting resistance to particular infectious diseases. These genetic variants leave "distinctive, detectable patterns of genetic variation in the human genome."[66] Also, they "may singly or in combination distinguish the members of one social group (an 'ethnic' group) from another."[67]

Toxin resistance may be among the genetic differences that could be exploited militarily. In a study published in 2011, researchers exposed anthrax bacterium cells from people of African, Asian, European, and North American descent (whose tissues were taken for a freely available genome database). Most of the cells fell to the assaults. However, cells from three people of European descent required hundreds or even thousands more times as much anthrax toxin to kill them. The researchers traced the broad range in anthrax sensitivity to regulating a specific gene (CMG2), which codes for a protein that controls anthrax's ability to access human cells.[68]

Another source of genetic variation is in the noncoding regions of the human genome. The technique of genetic fingerprinting, which dates back to the mid-1980s, can be used to identify regions in the noncoding DNA with a high rate of mutation—the so-called minisatellites. The minisatellites arise from mistakes in replication, and their unique patterns can be used to identify specific individuals. They can also be used to identify groups, as patterns of variation between individuals "is characteristic of a particular group and differs from group to group."[69]

Personal genomics companies like 23andMe collect genetic data through saliva-based, direct-to-consumer genetic testing and have already raised concerns about the prospect of Google-style data hoarding. A state or non-state actor could potentially apply the massive computational power to genomic databases, such as 23andMe and Ancestry.com, to design agents specific to individuals, a family, or a group.[70] The larger the group, the less precise the targeting. However, the most vulnerable populations would be those with minimum genetic diversity due to remaining mainly in their ancestral geographic regions with little outbreeding or

those that are genetically distinct even if dispersed. Among such populations may be Uighurs and Ashkenazi Jews.

One would not need individual genomes. Random DNA samples could be collected from sewer systems or subway cars, and they would provide an excellent genetic profile of a population. Coupling algorithms could further increase geographic and ethnic specificity for human DNA signatures (e.g., YES for sequence one, YES for sequence two, NO for sequence three, etc.) to target people with specific sequences but not others. This information could then be combined with DNA from the microbiome (gut) bacteria, which is also very specific in many dimensions. An ingested agent could sample the microbiome first and, if it is a match, enter the body and sample the host DNA.

The same principle could be applied to target crops and farm animals more efficiently than humans since most crops and farm animals are cloned or derived from a small group of prime breeders. Biosynthetic agents manufactured at a nanoscale could be mass-produced and include a high level of specificity. They would also not be alive, so they would not reproduce or reproduce only in specific hosts or conditions. These characteristics would limit both collateral and retroactive casualties.

By combining nanotechnology, computational power, and synthetic biology with AI and robotics, one can imagine a future involving various types of robots, drones, or satellites that could manufacture and deliver "smart germs" anywhere in real time.

In 2019, the US Department of Defense advised all military personnel against using direct-to-consumer genetic tests because they "could expose personal and genetic information, and potentially create unintended security consequences and increased risk to the joint force and mission."[71] It did not specify the unintended security consequences or increased risk.

Private DNA databases with identifying information could be hacked by (or sold to) malicious actors. Perhaps the Department of Defense worried that China was among those actors. Since 2017, the Chinese government has placed at least one million Uighurs and members of other minority groups in "prisonlike" detention centers "as part of a campaign to stop terrorism."[72] Hundreds of thousands of them were compelled to provide blood samples. Using their DNA (and with the help of American and European firms), the Chinese government is developing phenotyping technology that would predict someone's skin color, eye color, ancestry, and other features. Its current goal is to identify a person's physical appearance from a genetic sample alone.[73]

Experts worry that the phenotyping technology may be used not just for surveillance but also to "decide that someone does belong or does not belong" to a particular race or ethnicity.[74] It could also potentially be used to produce weapons that target individuals or groups based on characteristics such as skin color or ancestry.

Genetic editing could also enable delayed targeting, such as a particular group's or individual's future generations.[75] One possible mechanism for doing so may be the so-called gene drive. Gene drives allow propagating new genetic traits into or disabling an unwanted trait within the entire population not immediately but over a few generations. They can override standard molecular mechanisms of inheritance, thus ensuring that virtually all offspring inherit a newly engineered trait. The technique has been used mainly on sexually reproducing species with short life spans and numerous offspring, such as mosquitos and fruit flies. It would not work on bacteria or viruses because they reproduce asexually, but theoretically could be used on humans.[76] The Imperiale Framework describes the use of human gene drives as "impractical" because it relies on generations of sexual reproduction to spread a harmful trait, thus "warrant[ing] a minimal level of concern."[77]

Delayed targeting could take another form in the future. In 2003, the CIA requested that the National Academy of Sciences hold a closed seminar to consider the security implications of the recent and anticipated advances in genetic engineering. Among the scenarios the panel identified was a "stealth" virus that could be programmed to infect human cells and then remain dormant without provoking disease.[78] Stealth viruses exist in nature, with the notorious herpes virus a case in point. Engineered to be contagious and silently spread through the population years in advance, they would then "be activated by an internal or external signal and produce illness in infected individuals."[79] Or as one medical expert reckoned, a threat of activation could be used as blackmail.[80] The 2018 National Academy of Sciences report describes the stealth introduction of an engineered threat into the human microbiome as an area of "medium-high concern." Nevertheless, it also points out that, given our "nascent understanding" of the human microbiome, any targeted manipulation there would be difficult to detect or attribute.[81]

International Politics of Genetic Warfare

Just one week after the September 11 attacks, letters laced with anthrax began arriving at media and congressional offices. Coupled with the earlier revelations about the magnitude of the Soviet and Iraqi biowarfare pro-

grams, biological weapons came to be viewed as "one of the key security issues of the twenty-first century."[82] Two decades later, the specter of biowarfare reemerged. With the COVID-19 pandemic came the fear that "the invisible enemy can hide within our ranks, multiplying in secret, planting time bombs in our bodies, and all before we know what's hit us."[83]

The fear of secret genetic weapons capability and use is not limited to malicious non-state actors. In what has been characterized as a sign of "a new Cold War," a Chinese foreign ministry spokesman suggested in March 2020 that the US Army may have brought COVID-19 to Wuhan.[84] The US secretary of state responded in kind by alleging that the outbreak originated in a Chinese laboratory.[85] All the while, conspiracy theories about the origins of the disease spread on online platforms. Among them were the claims that the virus was part of China's "covert biological weapons program" and that a Canadian-Chinese spy team sent the virus to Wuhan.[86] Such undiplomatic exchanges and conspiratorial claims are particularly hazardous in the era of global competition among great powers.[87]

Biological weapons have always been more accessible than nuclear ones. However, with genetic engineering increasingly solving the problems of weaponization, delivery, and precision, Ebola expert Karl Johnson predicts that "any crackpot with a few thousand dollars' worth of equipment and a college biology education under his belt could manufacture bugs that would make Ebola look like a walk around the park."[88]

Predictions about genetic warfare would benefit from identifying the closest parallels and then adjusting and synthesizing the ensuing models. Genetic weapons have the destructive potential of nuclear weapons, but their ease of development is akin to cyber weapons. Both genetic and cyber warfare require inexpensive equipment and only a college-level understanding of these fields. Unlike nuclear weapons that demand enormous engineering expertise, a small team can develop and hone cyber and genetic weapons using common equipment.[89]

Dual-use capability is another similarity. Unlike nuclear and chemical weapons, genetically engineered bioweapons do not require equipment or materials exclusively tailored to their purpose. This concern was among the first raised in the US National Security Strategy in 2017.[90] As one military analyst stated, "A nuclear weapons facility has obvious signals to the outside world. We can look at it and immediately say, 'Ugh, that is a nuclear reactor. However, the technology for conducting biological weapons research is essentially the same as [for] what keeps a population healthy."[91] Many biological engineering techniques with dual-use potential are holy grails of medicine. Research journals publish techniques and results inter-

nationally, publicly, and without consideration for their security implications.[92] Dissemination of this information limits the effectiveness of the Biological Weapons Convention (BWC) and domestic control regimes.[93]

Biological weapons programs are far more challenging to detect than nuclear programs. They look like other biological research programs. The body charged with enforcing compliance with the BWC, the Implementation Support Unit, is significantly underfunded compared to the enforcement arms of the Chemical Weapons Convention and Non-Proliferation of Nuclear Weapons agreements. Much like for cyber weapons, custom bioweapon development is effectively unregulated.[94]

Genetic and cyber weapons are also similar in their strategic utility in terms of versatility, durability, and deniability. The scope and specificity of genetic weapons make them more analogous to cyber than any of the traditional weapons of mass destruction. Genetically engineered bioagents can achieve levels of specificity that were previously impossible using traditional pathogens. Targets can include ethnic groups and even specific individuals. They need not even be human: tailored pathogens can affect rubber, plastics, and other defense and infrastructure-related materials.[95] Similarly, cyberweapons can attack power grids and other nonhuman targets. Versatility, or the capacity to take on different forms of varying lethality against varied targets, makes genetic weapons potentially even more hazardous than nuclear weapons.

Finally, unlike nuclear, but similar to cyber, genetic weapons can be used covertly. Thus, those who employ them have plausible deniability. Much like North Korea proxies' use of ransomware or Russia's disinformation campaigns, a genetic weapon would be difficult to attribute. Even chemical weapons do not have this advantage. Attempts to deny their use, such as in Ghouta, Syria, typically fail miserably upon investigation.[96]

The ease of development and strategic benefits of genetic weapons make them, as one forecaster put it, "the most dangerous threat humanity has ever faced."[97] What would states and non-state actors do once they acquired them? Would they keep their genetic war capability secret? Would they use genetic weapons openly or covertly? These questions are considered next.

Genetic War Capability: Reveal or Conceal?

Underlying the question of whether to reveal or conceal genetic military capability is a trade-off. To conceal it is to gain a potent secret edge over rivals. To reveal it is to deter or frighten others from attacking.[98]

Deterrence works "because the expected reaction of the attacked will result in one's own severe punishment."[99] It is "the power to dissuade."[100]

Two factors determine whether actors reveal their clandestine capability, according to Brendan Rittenhouse Green and Austin Long.[101] The first is the uniqueness of the capability—the less unique, the less attractive is concealing relative to revealing. The second is the prospect that the adversary will implement countermeasures. Successful countermeasures can sharply degrade a weapon's military value.[102] The lower the odds of countermeasures, the more likely the actors are to reveal their clandestine capability.

The decision to reveal one's clandestine capability ultimately depends on one's need for deterrence. Traditional biological weapons could not deter because their outcome was always uncertain. However, without the problems of weaponizability, delivery, and precision plaguing them, genetic weapons could deter even countries with nuclear weapons. The destructive outcome of genetic weapons may be assured, immediate, and massive. A genetically engineered bioagent with a short incubation period could be released as instantly as a nuclear agent on a population of millions.[103] And, unlike nuclear weapons, which rely on city and civilian attacks, an attack by a genetic weapon is more likely to be militarily decisive—that is, to influence leaders' decisions about war and surrender. Its effects could inflict harm not only on civilians but also on the leaders themselves.[104] All of these factors make genetic weapons potentially more potent than nuclear weapons as a mechanism of deterrence.

Accordingly, state and non-state actors that need to demonstrate credible deterrence are most likely to reveal their genetic war capability. These actors lack the only other rivaling source of deterrence—nuclear weapons. Because they may be threatened or greedy, they are "willing to incur costs or risks for non-security expansion."[105] Nuclear states are the actors most disposed to conceal genetic war capability. They can reap the strategic benefits of hidden genetic power without worrying about survival-threatening aggression or retaliation.

Do the effects of genetic weapons need to be demonstrated for them to have a deterrence outcome similar to nuclear weapons? It may be that recent outbreaks, such as Ebola or COVID-19, provide the element of proof needed to convince a population and its political representatives of the credibility of the threat. The recent experience with outbreaks may instill, at least in the current generations, strong aversion and even fear. The collective memory of the atomic bombings of Hiroshima and Nagasaki, and even the Cold War–era duck-and-cover drills, has faded. However, the

memory of the COVID-19 pandemic is fresh and potent, especially for the generation that came of age during the pandemic.[106]

What makes genetic weapons unique is their combination of accessibility and destructive potential. Nuclear deterrence requires some evidence that an actor is capable of creating and delivering a nuclear weapon. However, with genetic weapons—including those the Imperiale Framework has deemed most urgent and concerning—no evidence of capability is necessary. Of itself, the accessibility of relevant technologies and know-how can portend a threat. A mere statement of one's willingness to use genetic weapons, combined with some signals of credibility of intention, may be enough to deter others from an attack. This possibility may be a dream for structural realists like Kenneth Waltz, if not for the accessibility of genetic weapons to states and non-state actors alike.[107]

Offensive Use: Open or Covert?

So too is there a trade-off between the open and covert use of genetic weapons. Covert use confers strategic and tactical benefits, such as surprise, deniability, and versatility. The benefits of unrestricted use are primarily psychological.

The overt use of genetic weapons can be thought of as a form of "costly signaling" or "actions so costly that bluffers and liars are unwilling to take them."[108] The strategic logics Barbara Walter and Andrew Kydd use to explain costly signaling by terrorist groups—specifically attrition, intimidation, and outbidding—are particularly productive here.[109] These logics rely mainly on psychological mechanisms. Actors engage in attrition to persuade their challenger that they are strong enough to impose costs if the latter continues the disliked course. Actors use intimidation to obtain compliance from others by signaling that they are strong enough to punish disobedience. Outbidding is used to demonstrate a superior resolve.[110] When it comes to using genetic weapons, it is also important to add ideological motivations to the list, especially genocidal and apocalyptic.

In sum, state and non-state actors are likely to use genetic weapons overtly for attrition, intimidation, and outbidding. They would also opt for unrestricted use to claim credit for genocide or ending the world. For everything else, there is covert genetic warfare.

Walter and Kydd specify the conditions under which the signaling mechanisms are likely to bear fruit. Attrition works best when adversaries are not deeply invested in the issue under dispute, are constrained in their ability to retaliate, and are highly sensitive to the costs of violence. Intimidation is effective on weak adversaries. Outbidding signals greater

commitment to the cause when the others are unwilling or unable to match the behavior.[111] The common theme is a relatively weak or politically constrained adversary. Given its invisible nature, open genetic warfare would affect a population physically and psychologically.[112] The ensuing hypothesis is that actors are more likely to openly use genetic weapons against an adversary that is militarily inferior and/or sensitive to the political fallout from the engagement. A militarily weak democratic state would make a prime target.

For some, genetic violence is not just a means but also an end. Genocidal regimes may consider genetic weapons a godsend. Such a prospect was not lost on CRISPR pioneer Jennifer Doudna, who describes a nightmare she had in which a colleague asked her to teach someone how her technology worked. She followed the colleague into a room to meet this person and "was shocked to see Adolf Hitler, in the flesh."[113]

Some actors with millenarian, apocalyptic beliefs might also welcome an open genetic war. These may include Protestant fundamentalist groups that anticipate an imminent end of history and embrace "radical violence" to hasten "the new heaven and the new Earth, the coming of the Kingdom of God."[114] Some jihadis, such as Islamic State of Iraq and Syria (ISIS) founder Abu Musab al-Zarqawi, also embrace the notion of end-times and extreme violence. Al-Zarqawi's brutality was so "unprecedented" that it shocked even al-Qaeda founder Osama bin Laden.[115] Many of the so-called new religious movements, or groups emerging outside the traditional religious categories, are similarly driven by the idea of a total transformation, though few of them embrace violence. Among those that do, Aum Shinrikyo's chemical and biological attacks in Tokyo suggest that millenarian cults could use genetic weapons secretly for tactical benefits. Violent racist, far-right groups may openly turn to genetic weapons to foment a "race war." Their fetishization of guns may, however, keep them away from biotechnology.

Conclusion

The development of biotechnology is rapid and decentralized. Hundreds of Manhattan projects may soon operate from inconspicuous laboratories around the world. How can we contain their security risks, which present an existential threat to humanity? The following options emerge: government regulation, government transparency, government-scientist collaboration, scientific transparency and self-governance, and norms. None is likely to work alone, but together they offer the best chance of preventing genetic war.

"I have not thought of that at all," Albert Einstein remarked when he first learned that the latest nuclear research discoveries, stemming from his famed equation $E = mc^2$, enabled the creation of an atomic bomb.[116] He then signed a letter warning President Franklin D. Roosevelt that Nazi Germany could develop nuclear weapons and suggested that the United States initiate its nuclear program. However, it was not Nazi Germany but the United States that dropped atomic bombs on hundreds of thousands of civilians.

In 1953, James Watson and Francis Crick revealed that the genome, which is the entirety of genetic information in any organism, is essentially digital. With the right tools, it can be decoded and edited. An early proponent of mapping the human genome, Watson recognized the need to address the policy implications of the endeavor. The Ethical, Legal and Social Implications (ELSI) program was thus set up as part of the Human Genome Project. The latter began in 1990 and, by 2003, successfully sequenced the 3 billion base pairs that compose human DNA. The goal of the corresponding ELSI program was, as Watson explained, "to address, anticipate, and develop suggestions for dealing with such [ethical, legal, and social] problems in order to forestall adverse effects."[117] The project's cosponsors, the National Institutes of Health and the US Department of Energy, spent over $100 million on ELSI research.[118] The ensuing work focused on potential discrimination by employers and health insurers, ethical standards for work with human research subjects and tissues, and controversial issues (e.g., cloning, stem cell research, and eugenics).[119] However, paralleling Einstein's initial approach to his research, the security risks of the new technologies were missing from the equation.[120]

What valuable lessons can we draw from the other weapons of mass destruction for limiting, or even preventing, the proliferation and use of genetic weapons? Considering what kept biological weapons from the battlefield in the twentieth century, medical anthropologist Jeanne Guillemin draws lessons from the nonuse of chemical weapons in World War II battlefields. Why did the Allied and Axis military commanders leave an entire class of armaments, tested in battle during World War I, on the shelf? Guillemin identifies four key factors: legal restraints, public opinion, technical drawbacks, and prospects of retaliation.[121] Could these prevent the development and use of genetic weapons?

The Biological and Toxin Weapons Convention, a Cold War–era treaty signed by the United States, China, Russia, and 176 other countries, bans the development of bioweapons. The previous treaty, the Geneva Protocol of 1925, prohibited chemical and biological weapons (but not their de-

velopment, production, and stockpiling). These treaties have, according to some, generated global norms that "clearly contributed to the fact that few countries have been engaged in research into offensive biowarfare during recent decades."[122]

Others argue that it was not norms generated by international treaties but the impracticalities of biological weapons that rendered them useless. And overcoming these impracticalities was just a matter of time. On the heels of World War II, bacteriologist Theodor Rosebury predicted that next time around, biological weapons would take center stage. He stated, "If World War III is allowed to come, biologists and men of all related fields, including physicians, will be called upon as never before to serve alongside physicists and other scientists as instruments of human destruction."[123] This prediction was puzzling because biological weapons were conspicuously absent during the Second World War. However, Rosebury reasoned that norms could prevent biological warfare no more successfully than they prevented the use of the crossbow or musket—both of which were, at some point, deemed weapons of cowards.[124] Technical impediments prevented biological warfare. And those were not "beyond the ken of human genius."[125]

Brian Mazanec considers the development of constraining norms in the domain of cyberspace. He finds that what causes norms to develop there is their alignment with the national interests of powerful states.[126] While we are witnessing the development of norms in cyber warfare thanks to the concerns of counties such as the United States, the chances of their internalization by everyone are meager.[127] The cyber warfare norms most likely to succeed are those that are limited in scope, such as focusing on applying the existing laws of armed conflict to cyber warfare or prohibiting the first use of cyber weapons.[128]

When it comes to the genome domain, one potential avenue for regulation and norms building lies in a focus on a critical ingredient: genetic data. Repurposing some general responses to data privacy concerns may help address the individual's rights to protect genetic information. A multipronged approach could borrow from national efforts such as the United States' Health Insurance Portability and Accountability Act (HIPAA) medical privacy laws or multijurisdictional protections such as the European Union's growing efforts to enshrine a "right to be forgotten." Also, policy makers could take complementary steps to grant individuals property rights to their genetic material or to utilize intellectual property protection schemes.

Because a research moratorium would be unrealistic, as the science and the technologies are global, the following are the options available for confronting the specter of genetic warfare. One is government transparency. As Guillemin concludes from her study of biological warfare, the threat of such weapons "increases in direct proportion to government secrecy, closed military cultures, and a subsequent lack of accountability to the public."[129] Another option is scientific transparency and self-governance. At a CIA-sponsored conference of life science experts that addressed the "darker bioweapons future," a panel suggested that the bioscience community would act "as a living sensor web at international conferences, in university labs, and through informal networks to identify and alert it to new technical advances with weaponization potential."[130]

Some advocate for more government-scientist collaboration. Most panelists at the CIA conference argued for a "qualitatively different relationship" between the government and life sciences communities. For example, the former could assist the latter in efforts to develop standards and norms to differentiate between "legitimate" and "illegitimate" research.[131] The US National Research Council Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology has, however, advised the US government not to attempt regulating scientific publishing. It argued that scientists and journal editors could screen their papers for security risks. With biological information and tools widely distributed, regulating only US researchers would have little effect.[132]

Optimism about transparency and self-governance characterizes many in the biotechnology community.[133] As one report summed up, "The scientific community historically has demonstrated its ability to lead the way in the responsible development of new technologies."[134] In 1975, scientists from around the world gathered in northern California at the famed Asilomar Conference Center to discuss the challenges presented by recombinant DNA technology. The technology permitted them to cut "long, unwieldy molecules of nucleotides into digestible sentences of genetic letters and paste them into other cells."[135] The scientists considered laboratory and environmental safety and concluded that the field required little regulation. There was no real discussion of deliberate abuse because "at the time, there didn't seem to be any need."[136]

This need now exists. The scientific community is currently debating what to do about the emerging technologies of the so-called Fourth Industrial Revolution," including biotechnology and gene editing. The community supports advancing biosecurity tools and practices like gene synthesis screening and keeping scientists informed about and involved in the

development of policies.[137] It also advocates that it is vital for the United States to collaborate with "equally capable and like-minded allies and partners," such as South Korea and India.[138] Some advise the United States to provide global leadership on safety standards while expanding security cooperation in the areas of global health, gene synthesis, and medical and pharmaceutical research.[139]

There is also essential work emphasizing the need for government regulation and a national strategy. The 2018 National Academies of Sciences report stresses the need for the government to develop new approaches to meet the new challenges while not abandoning the traditional tools for biological and chemical defense. For the former, it identifies the importance of nimble and adaptable strategies, given the rapid rates of technological change and uncertainty about which approaches an adversary might pursue.[140]

Drawing on the Imperiale Framework, Marcus Cunningham and John Geis propose a framework that prioritizes threats, regulates synthetic biology processes (not products) to guard against accidents and abuses, controls US technology exports, builds international cooperation, and conducts horizon scanning on machine learning.[141] They contend that the United States needs "a separate, comprehensive, whole-of-government national strategy." Further, the strategy must be globally exportable, as it "cannot be successful if America imposes unilateral restrictions on its activities that the rest of the world ignores or exploits."[142] Because it cannot wholly coerce or induce other states (and non-state actors) to adopt its model, the United States will also need to devote attention and resources to building global norms for new technologies in the coming decades. Such an effort would require a vast reservoir of soft power. SSQ

Acknowledgments

The author wishes to thank Brian Roberge and Jared Schwartz for research assistance, Bernard Possidente for guidance, and the Judith Johns Carrico Faculty Grant for supporting fieldwork.

Yelena Biberman

Dr. Biberman is an associate professor of political science at Skidmore College, a fellow at West Point's Modern War Institute, and a nonresident senior fellow at the Atlantic Council's South Asia Center. She is the author of *Gambling with Violence: State Outsourcing of War in Pakistan and India* (Oxford University Press, 2019).

Notes

1. Francis Fukuyama, *Our Posthuman Future: Consequences of the Biotechnology Revolution* (New York: Picador, 2002).

2. The term refers to the future Homo sapiens with God-like powers in Yuva Harari, *Homo Deus: A Brief History of Tomorrow* (New York: Random House, 2016).

3. Vladimir Putin, "Being Strong: National Security Guarantees for Russia," *Rossiiskaya Gazeta*, 28 February 2012, https://www.voltairenet.org/.

4. Putin.

5. Joby Warrick, "Putin Expands Secret Military Labs for 'Genetic' Bombs as Powerful as Nukes," *Miami Herald*, 19 March 2018, https://www.miamiherald.com/.

6. Marcus A. Cunningham and John P. Geis II, "A National Strategy for Synthetic Biology," *Strategic Studies Quarterly* 14, no. 3 (Fall 2020): 49–80, https://www.airuniversity.af.edu/.

7. James R. Clapper, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community Senate Armed Services Committee, 9* February 2016, 9, https://www.dni.gov/.

8. Clapper, 9.

9. National Academies of Sciences, Engineering, and Medicine (NASEM), *Biodefense in the Age of Synthetic Biology* (Washington, DC: The National Academies Press, 2018), 3, https://doi.org/10.17226/24890.

10. NASEM, 3–5.

11. Ben Westcott and Steven Jiang, "Chinese Diplomat Promotes Conspiracy Theory That U.S. Military Brought Coronavirus to Wuhan," CNN, 13 March 2020, https://www.cnn.com/; and Julian Borger, "Mike Pompeo: 'Enormous Evidence' Coronavirus Came from Chinese Lab," *Guardian*, 3 May 2020, https://www.theguardian.com/.

12. Gary Ackerman, "Chemical, Biological, Radiological and Nuclear (CBRN) Terrorism," in *Routledge Handbook of Terrorism and Counterterrorism*, ed. Andrew Silke (New York: Routledge, 2018).

13. Apocalyptic regimes are led by individuals who hold and/or strategically employ doomsday beliefs. For example, see William McCants, *The ISIS Apocalypse: The History, Strategy, and Doomsday Vision of the Islamic State* (New York: Picador, 2015).

14. Jeanne Guillemin, *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism* (New York: Columbia, 2005), 205.

15. The United States disavowed biological weapons in 1969. US president Richard Nixon characterized them as having "massive, unpredictable, and potentially uncontrollable consequences," such as pandemics and "impair[ing] the health of future generations." This was the first time a significant power unilaterally abandoned an entire weapon category. Nixon believed that biological weapons had limited tactical utility on the battlefield and were an unreliable strategic deterrent. He also calculated that public denunciation of biological weapons would make it easier for the US to retain its chemical weapons capability, which was of much greater value to the Pentagon. It would "dampen criticism of the ongoing U.S. combat use of tear gas and herbicides in Vietnam," which the Nixon administration intended to continue. Jonathan B. Tucker and Erin R. Mahan, *President Nixon's Decision to Renounce the U.S. Offensive Biological Weapons Program* (Washington, DC: National Defense University Press, October 2009), 10; and Brian M.

Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons* (Lincoln: University of Nebraska Press, 2015), 55.

16. Gigi Gronvall, "The Security Implications of Synthetic Biology," *Survival* 60, no. 4 (August–September): 170.

17. Andrew Moscrop, "Mass Hysteria Is Seen as Main Threat from Bioweapons," *British Medical Journal* 323, no. 3 (November 2001): 1023, https://www.ncbi.nlm.nih.gov/.

18. The list of obstacles is adapted from Theodor Rosebury, Elvin A. Kabat, and Martin H. Boldt, "Bacterial Warfare, A Critical Analysis of the Available Agents, Their Possible Military Applications, and the Means for Protection Against Them," *Journal of Immunology* 56, no. 1 (May 1947): 7–96, https://europepmc.org/.

19. British Medical Association, *Biotechnology, Weapons and Humanity* (Australia: Harwood Academic Publishers, 1999), 3.

20. Sonia Ben Ouagrham-Gormley, *Barriers to Bioweapons: The Challenges of Expertise and Organization for Weapons Development* (Ithaca, NY: Cornell University Press, 2014), 5.

21. Ben Ouagrham-Gormley, 5–6.

22. Gigi Kwik Gronvall et al., *The Industrialization of Biology and Its Impact on National Security* (Pittsburgh: Center for Biosecurity of UPMC [University of Pittsburgh Medical Center], 8 June 2012), 1, https://www.centerforhealthsecurity.org/; and Kathleen M. Vogel, "Intelligent Assessment: Putting Emerging Biotechnology Threats in Context," *Bulletin of the Atomic Scientists* 69, no. 1 (2013): 45, https://doi.org/10.1177%2F0096340212470813.

23. NASEM, *Biodefense in the Age of Synthetic Biology*, 7–8.

24. Cunningham and Geis, "National Strategy for Synthetic Biology," 50.

25. Eric D. Green, Edward M. Rubin, and Maynard V. Olson, "The Future of DNA Sequencing," *Nature* 550 (October 2017): 179–81, https://doi.org/10.1038/550179a.

26. Green, Rubin, and Olson, 179–81.

27. Green, Rubin, and Olson, 179–81.

28. Stacey Pereira, Richard A. Gibbs, and Amy L. McGuire, "Open Access Data Sharing in Genomic Research," *Genes* 5, no. 3 (2014): 739–4, https://doi.org/10.3390/genes5030739.

29. An example of this is the FAIR (Findability, Accessibility, Interoperability, and Reusability) Principles for genomic data sets. Mark D. Wilkinson et al., "The FAIR Guiding Principles for Scientific Data Management and Stewardship," *Scientific Data* 3 (March 2016), https://doi.org/10.1038/sdata.2016.18.

30. Yaniv Erlich and Dina Zielinski, "DNA Fountain Enables a Robust and Efficient Storage Architecture," *Science* 355, no. 6328 (March 2017): 950, https://doi.org/10.1126/science.aaj2038.

31. For more on the strategic implications of AI, see James S. Johnson, "Artificial Intelligence: A Threat to Strategic Stability," *Strategic Studies Quarterly* 14, no. 1 (Spring 2020): 16–39, https://www.airuniversity.af.edu/.

32. Raquel Dias and Ali Torkamani, "Artificial Intelligence in Clinical and Genomic Diagnostics," *Genome Medicine* 11, no. 70 (2019): 4, https://genomemedicine.biomedcentral.com/.

33. Dias and Torkamani, 4.

34. CRISPR researcher (Cold Spring Harbor Laboratory, NY), interview by the author, October 2017.

35. Alan Yu, "How a Gene Editing Tool Went from Labs to a Middle-School Classroom," NPR, 27 May 2017, https://www.npr.org/.

36. Rachel M. West and Gigi Kwik Gronvall, "CRISPR Cautions: Biosecurity Implications of Gene Editing," *Perspectives in Biology and Medicine* 63, no. 1 (Winter 2020): 74, doi:10.1353/pbm.2020.0006.

37. Clapper, *Statement for the Record*, 6.

38. Puping Liang et al., "CRISPR/Cas9-Mediated Gene Editing in Human Tripronuclear Zygotes," *Protein Cell* 6, no. 5 (2015): 363–72, https://pubmed.ncbi.nlm.nih.gov/.

39. Hong Ma et al. "Correction of a Pathogenic Gene Mutation in Human Embryos," *Nature* 548 (24 August 2017): 413–19, https://doi.org/10.1038/nature23305.

40. Giorgia Guglielmi, "First CRISPR Test for the Coronavirus Approved in the United States," *Nature*, 8 May 2020, https://www.nature.com/.

41. I thank Bernard Possidente for suggesting this useful analogy.

42. Cunningham and Geis, "National Strategy for Synthetic Biology," 52–53.

43. Jeronimo Cello, Aniko V. Paul, and Eckard Wimmer, "Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template," *Science* 297, no. 5583 (August 2002):1016–18, https://science.sciencemag.org/.

44. George Church and Ed Regis, *Regenesis: How Synthetic Biology Will Reinvent Nature and Ourselves* (New York: Basic Books, 2014), 2.

45. Church and Regis, 4.

46. Eric Young and Hal Alper, "Synthetic Biology: Tools to Design, Build, and Optimize Cellular Processes," *Journal of Biomedicine and Biotechnology,* 2010, 1, https://doi.org/10.1155/2010/130781. For example, see Deborah A. Weighill et al., "Multi-Phenotype Association Decomposition: Unraveling Complex Gene-Phenotype Relationships," *Frontiers in Genetics* 10 (2019), https://doi.org/10.3389/fgene.2019.00417. For a review of possible options, see Nadia Solovieff et al., "Pleiotropy in Complex Traits: Challenges and Strategies," *Nature Reviews Genetics* 14, no. 7 (July 2013): 483–95, https://doi.org/10.1038/nrg3461.

47. Peter Kornbluh, ed., "Oscars: 'Bridge of Spies,' The Sequel," Briefing Book 542 (Washington, DC: National Security Archives, 26 February 2016), https://nsarchive.gwu.edu/.

48. William Rosenau, "Aum Shinrikyo's Biological Weapons Program: Why Did It Fail?," *Studies in Conflict & Terrorism* 24, no. 4 (2001): 296–97, https://doi.org/10.1080/10576100120887.

49. Rosenau, 296–97.

50. Edmond Hooker, "Biological Warfare," emedicinehealth, 10 January 2019, https://www.emedicinehealth.com/.

51. Ben Ouagrham-Gormley, *Barriers to Bioweapons*.

52. Catherine Jefferson, Filippa Lentzos, and Claire Marris, "Synthetic Biology and Biosecurity: Challenging the 'Myths,'" *Frontiers in Public Health* 2, article 115 (August 2014): 10, https://doi.org/10.3389/fpubh.2014.00115.

53. Yaojun Tong et al., "Highly Efficient DSB-Free Base Editing for Streptomycetes with CRISPR-BEST," *Proceedings of the National Academy of Sciences of the United States of America* 116, no. 41 (8 October 2019): 20366–75, https://doi.org/10.1073/pnas.1913493116.

54. Sean C. Sleight and Herbert M. Sauro, "Design and Construction of a Prototype CMY (Cyan-Magenta-Yellow) Genetic Circuit as a Mutational Readout Device to

Measure Evolutionary Stability Dynamics and Determine Design Principles for Robust Synthetic Systems," *Artificial Life* 13 (2012): 486, https://direct.mit.edu/.

55. Yen-Hsiang Wang, Kathy Y. Wei, and Christina D. Smolke, "Synthetic Biology: Advancing the Design of Diverse Genetic Systems," *Annual Review of Chemical and Biomolecular Engineering* 4 (2013): 20, https://doi.org/10.1146/annurev-chembioeng-061312-103351.

56. A single nanometer is about one half the width of a DNA molecule.

57. NATO, *NATO 2020: Assured Security; Dynamic Engagement – Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO* (Brussels: NATO Public Diplomacy Division, 17 May 2010), 15, https://www.nato.int/.

58. Margaret E. Kosal, "The Security Implications of Nanotechnology," *Bulletin of the Atomic Scientists* 66, no. 4 (July–August 2010): 63, https://doi.org/10.2968/066004006.

59. "Experts Warn of New Weapons through Nanotechnology," *Nuclear Threat Initiative*, 24 May 2005, https://www.nti.org/.

60. Evan J. Wallach, "A Tiny Problem with Huge Implications – Nanotech Agents as Enablers or Substitutes for Banned Chemical Weapons: Is a New Treaty Needed?," *Fordham International Law Journal* 33, no. 3 (2009): 862, https://ir.lawnet.fordham.edu/.

61. Jeff Daniels, "Mini-Nukes and Mosquito-Like Robot Weapons Being Primed for Future Warfare," *CNBC*, 17 March 2017, https://www.cnbc.com/.

62. Nikolay Kornienko et al., "Interfacing Nature's Catalytic Machinery with Synthetic Materials for Semi-Artificial Photosynthesis," *Nature Nanotechnology* 13 (October 2018): 890–99, https://doi.org/10.1038/s41565-018-0251-7.

63. Carl A. Larson, "Ethnic Weapons," *Military Review* 50, no. 11 (November 1970): 4, https://www.armyupress.army.mil/.

64. British Medical Association, *Biotechnology, Weapons and Humanity* (Australia: Harwood Academic Publishers, 1999), 63.

65. Pardis C. Sabeti, "Natural Selection: Uncovering Mechanisms of Evolutionary Adaptation to Infectious Disease," *Nature Education* 1, no. 1 (2008): 13, https://www.nature.com/.

66. Sabeti, 13.

67. British Medical Association, *Biotechnology, Weapons and Humanity*, xviii.

68. Martchenko et al., "Human Genetic Variation Altering Anthrax Toxin Sensitivity," *Proceedings of the National Academy of Sciences* 109, no. 8 (2011): 2972–77, https://doi.org/10.1073/pnas.1121006109.

69. British Medical Association, *Biotechnology, Weapons and Humanity*, 64.

70. Christopher Lane, "Personalized Genomics, Data-Hoarding, and Drug Companies," *Psychology Today*, 14 January 2015.

71. Joseph D. Kernan and James N. Stewart, Office of the Secretary of Defense, Memorandum, Subject: Direct-to-Consumer Genetic Testing Advisory for Military Members, 20 December 2019.

72. Sui-Lee Wee and Paul Mozur, "China Uses DNA to Map Faces, with Help from the West," *New York Times*, 3 December 2019, https://www.psychologytoday.com/.

73. Wee and Mozur.

74. Interview of Yves Moreau by Scott Simon, "Uighurs and Genetic Surveillance in China," NPR, 7 December 2019, https://www.npr.org/.

75. Andrew Goliszek, *In the Name of Science: A History of Secret Programs, Medical Research, and Human Experimentation* (New York: St. Martin's Press, 2003), 261.

76. "Gene Drives," SciLine, American Association for the Advancement of Science, 18 April 2018, https://www.sciline.org/.

77. NASEM, *Biodefense in the Age of Synthetic Biology*, 4.

78. Nuclear Threat Initiative, "U.S. Scientists Warn CIA of New 'Designer' Biological Agents," 17 November 2003, https://www.nti.org/.

79. Francisco Galamas, "Biological Weapons, Nuclear Weapons and Deterrence: The Biotechnology Revolution," *Comparative Strategy* 27, no. 4 (2008): 320–321, https://doi.org/10.1080/01495930802358364.

80. Michael J. Ainscough, "Next Generation Bioweapons: Genetic Engineering and Biological Warfare," in *The Gathering Biological Warfare Storm,* eds. Jim A. Davis and Barry R. Schneider (Westport, CT: Praeger, 2004), 180, https://www.nti.org/.

81. NASEM, *Biodefense in the Age of Synthetic Biology,* 74.

82. Gregory Koblentz, "Pathogens as Weapons: The International Security Implications of Biological Warfare," *International Security* 28, no. 3 (Winter 2003/04): 84, https://www.belfercenter.org/.

83. Max Brooks, "The Next Pandemic Might Not Be Natural," *Foreign Policy*, 20 April 2020, https://foreignpolicy.com/.

84. John Haltiwanger, "The US and China Are on the Brink of a New Cold War That Could Devastate the Global Economy," *Business Insider Australia*, 13 May 2020, https://www.businessinsider.com/; and Westcott and Jiang, "Chinese Diplomat Promotes Conspiracy Theory."

85. Borger, "Mike Pompeo."

86. Shayan Sardarizadeh and Olga Robinson, "Coronavirus: U.S. and China Trade Conspiracy Theories," BBC, 26 April 2020, https://www.bbc.com/.

87. Cunningham and Geis, "National Strategy for Synthetic Biology," 50.

88. Quoted in Brooks, "Next Pandemic Might Not Be Natural."

89. Frank Jordans, "Clinton Warns of Bioweapon Threat from Gene Tech," NBC News, 7 December 2011.

90. Donald J. Trump, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 9, https://trumpwhitehouse.archives.gov/.

91. Baumgaertner and Broad, "North Korea's Less-Known Military Threat."

92. Michael J. Selgelid, "Governance of Dual-Use Research: An Ethical Dilemma," *Bulletin of the World Health Organization* 87 (2009): 720–23, https://www.ncbi.nlm.nih.gov/.

93. Edgar J. DaSilva, "Biological Warfare, Bioterrorism, Biodefence and the Biological and Toxin Weapons Convention," *Electronic Journal of Biotechnology* 2, no. 3 (December 2019), http://www.ejbiotechnology.info/.

94. R. Daniel Bressler and Chris Bakerlee, " 'Designer Bugs': How the Next Pandemic Might Come from a Lab," Vox, 6 December 2018, https://www.vox.com/.

95. Jan van Aken and Edward Hammond, "Genetic Engineering and Biological Weapons," *EMBO Reports* 4, no. S1 (2003): 57–60, https://doi.org/10.1038/sj.embor.embor860.

96. Human Rights Watch, "Attacks on Ghouta: Analysis of Alleged Use of Chemical Weapons in Syria," 10 September 2013, https://www.hrw.org/.

97. Brooks, "Next Pandemic Might Not Be Natural."

98. Brendan Rittenhouse Green and Austin Long, "Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition," *International Security* 44, no. 3 (Winter 2019/20): 50, https://direct.mit.edu/.

99. Kenneth Waltz, "The Spread of Nuclear Weapons: More May Better," *Adelphi Papers* 171 (London: International Institute for Strategic Studies, 1981), https://www.mtholyoke.edu/.

100. Glenn H. Snyder, "Deterrence and Defense," in *The Use of Force: International Politics and Foreign Policy,* eds. Robert J. Art and Kenneth N. Waltz (New York: University Press of America, 1983), 129.

101. Green and Long, "Conceal or Reveal?," 50.

102. Green and Long, 51.

103. Galamas, "Biological Weapons," 317.

104. Ward Wilson, "The Myth of Nuclear Deterrence," *Nonproliferation Review* 15, no. 3 (November 2008): 423, https://www.nonproliferation.org/.

105. Charles L. Glaser, "Political Consequences of Military Strategy: Expanding and Refining the Spiral and Deterrence Models," *World Politics* 44, no. 4 (July 1992): 501, https://www.jstor.org/.

106. As Stephen Rosen observes, while "historical episodes will mark most clearly the men and women who lived through them," young individuals are marked the most by events. This is because "old people have many memories of the past, but new short-term memories are not formed as easily as when young. Young people will not be generally afraid, but when they are afraid, they will react very strongly, and so they will be capable of forming new memories easily." Stephen Peter Rosen, *War and Human Nature* (Princeton, NJ: Princeton University Press, 2005), 52.

107. Kenneth Waltz, "Why Iran Should Get the Bomb," *Foreign Affairs* 91, no. 4 (July/August 2012): 2–5, https://www.foreignaffairs.com/.

108. Andrew H. Kydd and Barbara F. Walter, "The Strategies of Terrorism," *International Security* 31, no. 1 (Summer 2006): 58, https://www.belfercenter.org/.

109. Kydd and Walter, 51.

110. Kydd and Walter, 51.

111. Kydd and Walter, 60, 67, 77.

112. Galamas, "Biological Weapons," 317.

113. Jennifer A. Doudna and Samuel H. Sternberg, *A Crack in Creation: Gene Editing and the Unthinkable Power to Control Evolution* (Boston: Houghton Mifflin Harcourt, 2017), 199.

114. Thomas Lecaque, "The Apocalyptic Myth That Helps Explain Evangelical Support for Trump," *Washington Post*, 26 November 2019, https://www.washingtonpost.com/.

115. Leon Aron, "Kingdom Come: Millenarianism's Deadly Allure, from Lenin to ISIS," *New York Review of Books*, 13 February 2018 https://www.nybooks.com/.

116. William Lanouette, *Genius in the Shadows: A Biography of Leo Szilard, the Man Behind the Bomb* (New York: Skyhorse Publishing, 2013), 205.

117. Lauren McCain, "Informing Technology Policy Decisions: The US Human Genome Project's Ethical, Legal, and Social Implications Programs as a Critical Case," *Technology in Society* 24, nos. 1–2 (2002): 112, https://www.sciencedirect.com/.

118. McCain, "Informing Technology Policy Decisions."

119. National Human Genome Research Institute, "Ethical, Legal and Social Issues in Genomic Medicine," accessed July 2021, https://www.genome.gov/.

120. For example, see testimonies at *The Science and Ethics of Genetically Engineered Human DNA, Hearing before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives*, 114th Cong., 1st sess., 16 June

2015 (Washington, DC: Government Printing Office, 2016), https://www.govinfo.gov/. While all of the participants acknowledged that gene editing raises important "ethical" considerations and called for regulations, none directly tackled its national and international security implications.

121. Guillemin, *Biological Weapons*, viii.

122. Aken and Hammond, "Genetic Engineering and Biological Weapons," 59.

123. Theodor Rosebury, *Peace or Pestilence: Biological Warfare and How to Avoid It* (New York: Whittlesey House, 1949), 183.

124. Rosebury, 178.

125. Rosebury, 116.

126. Mazanec, *Evolution of Cyber War*, 6.

127. Mazanec, 2.

128. Mazanec, 6–7.

129. Guillemin, *Biological Weapons*, 204.

130. Central Intelligence Agency (CIA), "The Darker Bioweapons Future," 3 November 2003, 2, https://fas.org/.

131. CIA, 2.

132. National Research Council of the National Academies, Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, *Biotechnology Research in an Age of Terrorism: Confronting the Dual-Use Dilemma* (Washington, DC: The National Academies Press, 2003), https://www.nap.edu/

133. Author's interviews at Bio-IT World Conference, Boston, MA, 15–17 May 2018.

134. National Research Council of the National Academies, *Biotechnology Research in an Age of Terrorism*, vii.

135. Michael Specter, "A Life of Its Own: Where Will Synthetic Biology Lead Us?," *New Yorker*, 28 September 2009, https://www.newyorker.com/.

136. Specter.

137. Amanda Kobokovich et al., "Strengthening Security for Gene Synthesis: Recommendations for Governance," *Health Security* 17, no. 6 (2019): 427, https://doi.org/10.1089/hs.2019.0110; and Gigi Kwik Gronvall, "Safety, Security, and Serving the Public Interest in Synthetic Biology," *Journal of Industrial Microbiology and Biotechnology* 45, no. 7 (July 2018): 463, https://doi.org/10.1007/s10295-018-2026-4.

138. Vaughan Turekian et al., *Building a Smart Partnership for the Fourth Industrial Revolution* (Washington, DC: Atlantic Council, April 2018), 1, https://www.atlanticcouncil.org/; and Gigi Kwik Gronvall et al., *US-India Strategic Dialogue on Biosecurity: Report on the Sixth Dialogue Session* (Baltimore: Johns Hopkins Center for Health Security, June 2019), https://www.centerforhealthsecurity.org/.

139. Gigi Kwik Gronvall, "Chapter 3: Ensuring Biosafety and Security," in Turekian et al., *Building a Smart Partnership for the Fourth Industrial Revolution*, 30.

140. NASEM, *Biodefense in the Age of Synthetic Biology*, 126.

141. Cunningham and Geis, "National Strategy for Synthetic Biology," 60–71.

142. Cunningham and Geis, 50, 71.