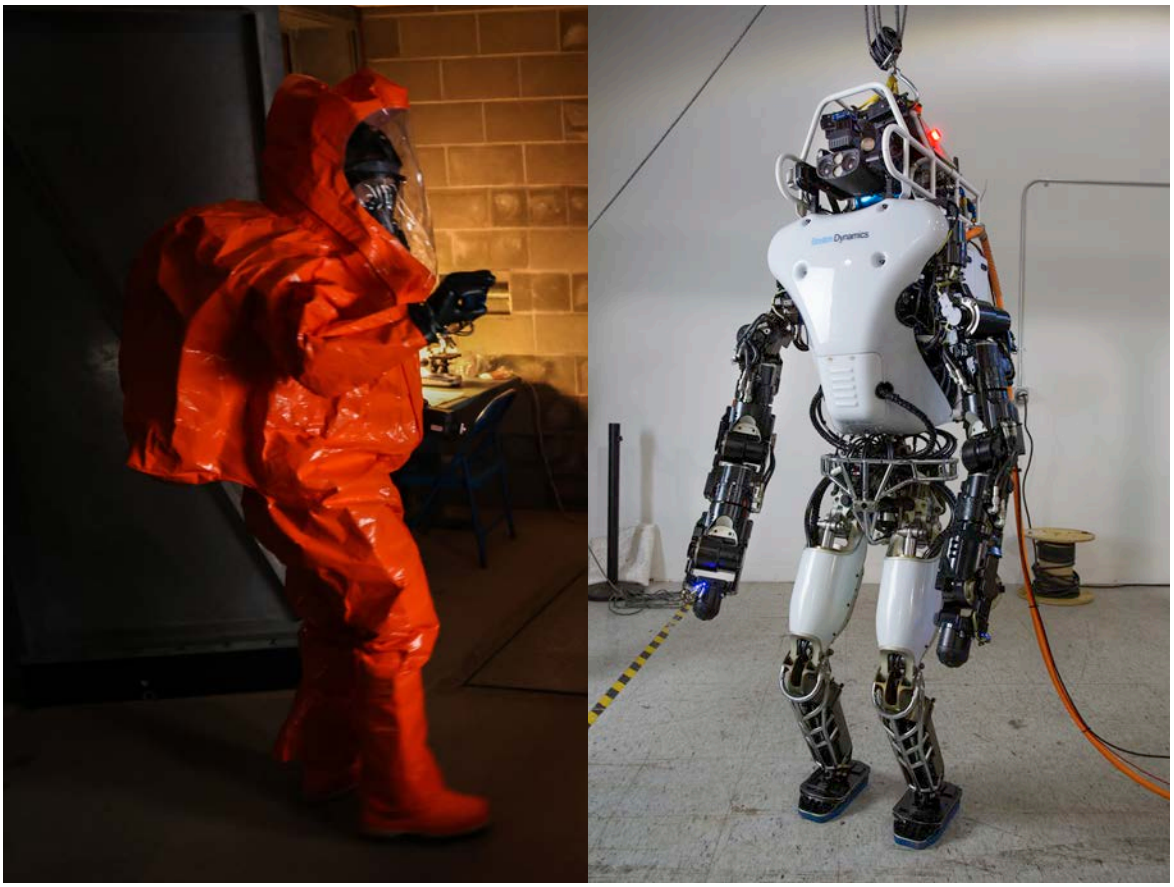
RAND CORPORATION

Research Report

LUKE J. MATTHEWS, MARY LEE, BRANDON DE BRUHL, DANIEL ELINOFF, CHRISTOPHER A. EUSEBI

Plagues, Cyborgs, and Supersoldiers

The Human Domain of War



For more information on this publication, visit **www.rand.org/t/RRA2520-1**.

About RAND

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-1254-6

Cover photo: Jason Kriess /U.S. National Guard and Worcester Polytechnic Institute/DARPA.

Limited Print and Electronic Distribution Rights

About This Report

Advances in biotechnology within the past half decade have renewed questions about the use of biotechnologies in a warfighting context. Prior to advances of the past few years and with respect to nation-states, biological weapons were usually deemed too liable to inflict harm on one's own forces to be of much strategic value; past military applications of genomics are viewed largely as misguided eugenicist pseudoscience; and, until recently, such technologies as brain-computer interfaces (BCI) were too unwieldy for the battlefield. As of this writing in 2023, technological improvements—including messenger ribonucleic acid (mRNA) vaccines, the use of CRISPR (clustered regularly interspaced short palindromic repeats) gene sequences as genetic engineering tools, and advances in BCI—and their accessibility to both friendly forces and adversaries—could shift these strategic calculations. This report explores how recently achieved or likely future technologies change strategic choices for the human body as a warfighting domain.

The analyses and recommendations in this report should be of interest to policymakers in the biotechnology, defense, and intelligence communities, as well as to a general audience.

RAND National Security Research Division

This research was sponsored by the Office of the Secretary of Defense and conducted within the Acquisition and Technology Policy Program of the RAND National Security Research Division (NSRD), which operates the National Defense Research Institute (NDRI), a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND Acquisition and Technology Policy Program, see www.rand.org/nsrd/atp or contact the director (contact information is provided on the webpage).

Acknowledgments

We thank Barry Pavel for his guidance and for supporting this work, as well as our RAND colleagues, Chris Mouton, Yun Kang, Caitlin Lee, Michael Spirtas, and Zachary Pandl of NSRD. We also thank Edward You of the Office of the Director of National Intelligence for sharing his insights. We are grateful to our RAND colleague Richard Silberglitt for his help with our Internet of Bodies patent analysis. We also thank RAND colleagues Tim Bonds, Marjory Blumenthal, Christy Foran, Alison Hottes, Don Prosnitz, Todd Richmond, Jon Schmid, and Tricia Stapleton, as well as the RAND Pardee Graduate School Technology and Narrative Laboratory Conclave for fruitful discussions.

Many thanks to Sydne Newberry for helping to edit and improve the clarity of this report and to Rachel Widom for formatting it. We are grateful to Marjory Blumenthal and Christy Foran for their thoughtful reviews of an earlier draft of this report.

Contents

Figures and Tables

Figures

Tables

Chapter 1

Introduction

Recent advances in biotechnology have renewed questions about the use of biotechnologies in a warfighting context. In the past, biological weapons were thought to present too great a risk of inflicting harm on friendly forces to be of much strategic value (Department of Homeland Security, 2023; Mauroni, 2022); past military applications of genomics are viewed largely as misguided eugenicist pseudoscience (Roll-Hansen, 2010); and, until recently, such technologies as brain-computer interfaces (BCIs) were too unwieldy for the battlefield (Binnendijk, Marler, and Bartels, 2020; Tucker, 2023). Today, technological improvements, including messenger ribonucleic acid (mRNA) vaccines, the use of CRISPR (clustered regularly interspaced short palindromic repeats) gene sequences as a genetic engineering tool, and advances in BCI, may shift these strategic calculations. The emergence of ever more countries with advanced biotechnology capabilities raises a new, more dynamic future for biotechnology at war. While these visions of the future might seem fantastical, we need only consider the great conflicts of the 20th century to see how biotechnology played pivotal roles as both weapons and cures. Given the rapid advancements brought about by the 21st-century biotechnology revolution, the application of artificial intelligence (AI) algorithms, and advanced human-machine systems, we see a complex, high-threat landscape emerging where future wars are fought with humans controlling hyper-sophisticated machines with their thoughts; the military-industrial base is disturbed by synthetically generated, genomically targeted plagues; and the future warfighter goes beyond the baseline genome to become an enhanced warfighter who is capable of survival in the harshest of combat environments. In this report, we explore how recently achieved or likely future technologies change strategic choices for the human body as a warfighting domain.

Motivation for This Research

Consider the scenario described in Vignette 1.

Vignette 1: Pandemic Land Grab

In September 2028, a previously unknown coronavirus begins to spread across countries in the South China Sea. Public health officials find that the virus is different enough from severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2)—which caused the coronavirus disease 2019 (COVID-19) pandemic—that the new virus is granted its own designation as SARS-CoV-3. It easily evades immunity from prior COVID-19 infections and vaccinations and is exacerbated in spread by the ongoing monsoon season that keeps people indoors. It then appears, near-simultaneously, on multiple U.S. Navy vessels, forcing most of the *Nimitz* carrier strike group to cease operations. Officials at the Centers for Disease Control and Prevention (CDC), the Department of Defense (DoD), and the Central Intelligence Agency begin a bureaucratic turf battle over which agency is best suited to investigate whether or not the shutdown of naval forces is due to an infectious agent of wholly natural origins. Regardless, with the U.S. naval response compromised and Taiwan having enforced stringent SARS-CoV-3 control measures, the Chinese military mounts an assault on Taiwan in the first week of October as the rains clear, and its military captures the island in 46 hours. The new virus is spreading slowly among the Chinese population and is curiously absent among the Chinese military and military supply-chain workers. The World Health Organization (WHO) highlights this as evidence for the success of Chinese social distancing procedures. What the WHO does not know is that since late 2027, nearly all members of the Chinese military—and roughly half the Chinese population—has been unwittingly vaccinated for SARS-CoV-3 under the pretense of a standard COVID-19 booster campaign.

Vignette 1 is science fiction, but it is not far-fetched. Although it remains unresolved whether genetic manipulations, such as gain-of-function research or an unintentional lab leak,[1] played a role in the origins of SARS-CoV-2, advances in biotechnology make it straightforward for any suitably trained and equipped laboratory to produce coronaviruses—or other pathogens—that will escape immunity from prior infections or vaccines.

The COVID-19 pandemic enabled the first test of mRNA vaccine technology, which facilitates much faster vaccine design and production than afforded by prior techniques. The mRNA technology allowed the vaccine for COVID-19 to be developed within a single year, whereas the previous record was four years for the development of the mumps vaccine (Ball, 2020). The facts that (1) pathogens can be engineered to escape immunity and (2) mRNA vaccines can be rapidly developed introduce the potential for strategic use of bioweapons that previously would have been much less tractable. From a purely technical standpoint, at this time, many countries could engineer pathogens to infect others while rendering their own populations immune through mRNA vaccines. The use of a coronavirus bioweapon in the scenario described in Vignette 1 could make rational strategic sense for such U.S. adversaries as the Chinese government because such a weapon might be able to paralyze U.S. naval responses without incurring the military cost from a U.S. response to an opening salvo of kinetic strikes against the U.S. military. This is possible because the origins of an engineered pathogen would be highly uncertain, scientists would likely presume natural *zoonosis* (crossing from animals to humans) as the simplest explanation, and it would take years of research to ascertain the origin empirically. This ambiguity could serve a nation-state well in a scenario like Vignette 1, especially considered in contrast to the lack of ambiguity once a country begins kinetic strikes against the U.S.

[1] *Gain-of-function research* refers to intentional laboratory-induced genomic mutations aimed at increasing the infectivity or lethality of microorganisms, such as viruses or bacteria, to their hosts.

Navy. A bioweapon of ambiguous origin could be a strategically valuable way to degrade an adversary's capabilities in advance of the onset of kinetic actions. This strategy is similar to the coupling of cyberattacks with subsequent kinetic attacks. Because the attribution of cyberattacks is difficult, adversaries can take advantage of the confusion by following with a kinetic attack (Libicki, 2020). This occurred in the Russia-Georgia war in 2008, when a kinetic attack was preceded by a distributed denial-of-service attack against Georgian military communications (Libicki, 2020).

In what follows, we outline additional scenarios—some that are near term and high-probability and some longer term and more speculative—for advances in engineered bioweapons, the Internet of Bodies (IoB),[2] and genomics. But first, we consider the definitional question of the extent to which the human body is a distinct domain of warfighting.

Defining the Human Body as a Warfighting Domain

The China-Taiwan scenario described in Vignette 1 postulates that an engineered bioweapon could be used in close coordination with actions in other domains (e.g., sea and air) to achieve a strategic goal (e.g., conquest of Taiwan). Warfighting domains are conceived as spatial or virtual places in which conflict can take place. Land, sea, and air are the traditionally recognized warfighting domains (space having been added in the past decade). Whether other zones of warfare, such as cyber, constitute *domains* is contested by researchers and strategists (Doherty, 2015; Egloff, 2022; McGuffin and Mitchell, 2014).

But can the human body itself be a warfighting domain? Can the body be an offensive or defensive weapon or a very specialized kind of target? As one approach to understanding the ways in which the human body might or might not be a distinct domain of warfighting, our team identified domain features mentioned in the research literature on warfighting domains and then assigned proposed domains for each of the features (Table 1.1).

[2] The *Internet of Bodies* (IoB) is the ecosystem of internet-connected devices collecting biometric or person-generated health data about an individual, together with the data it collects (Lee et al., 2020; see also Matwyshyn, 2019). The IoB includes but is not limited to technologies that connect the human body to an online network via devices that are connected to the body in some way, either by virtue of having been swallowed, implanted, or worn, so that the body can be monitored or controlled remotely. The IoB is part of the Internet of Things, and individuals whose capabilities are enhanced through IoB are *cyborgs* under most dictionary definitions for this term.

Table 1.1. Features of Putative Warfighting Domains

Putative Domain	Domain Features				
	Domain-Specific Human Movement and Survival Constraints	Domain-Specific Attack Modes	Observed Intra-Domain Escalation Without Cross-Domain Escalation	Observed Warfare[a] Within Domain	Domain-Specific Personnel and Skills
Land	Yes	Yes	Yes	Yes	Yes
Sea	Yes	Yes	Yes	Yes	Yes
Air	Yes	Yes	Yes	Yes	Yes
Space	Yes	Yes	?	No	Yes
Cyber	N/A	Yes	Yes	No	Yes
Intelligence	N/A	Yes	Yes	No	Yes
Human body	N/A	Yes	No[b]	Yes	?[c]

[a] By *warfare*, we mean the generally accepted understanding of it as "a conflict between political groups involving hostilities of considerable duration and magnitude" ("War: The Causes of War," undated). Such a definition does not require that those hostilities always be lethal, but it does require that they have a duration (i.e., a beginning and an end that are notably distinct from normal relations between the relevant political groups). In other words, uses of even lethal violence between political groups might not be warfare if they do not constitute a notably increased level of hostilities for a definable duration.

[b] We are unaware of any clear cases of domain-specific escalation, such as exchanges of attacks via engineered pathogens between nation-states, in the published literature. Such escalation, however, is conceivable.

[c] Medical professionals might be considered as human-body-domain–specific personnel, but they also might be regarded as personnel components of the traditional domains.

NOTE: N/A = not applicable.

Table 1.1 highlights one feature of traditional warfighting domains (land, sea, and air) that is inapplicable to such domains as cyber or the human body; that is, requiring particular modalities for human movement and survival. In other words, humans must be able to move, operate, and survive in these traditional domains, and the methods to do so must be compatible within that domain. If this feature is taken as necessary for something to constitute a domain, then by definition of the more newly proposed domains (space, cyber, intelligence, and the human body), only space can be considered a domain. Analysis arguing for space as a warfighting domain generalizes from the traditional land, sea, and air domains by noting that, although few humans may move through, fight in, or die in space, space still involves movement through a distinct spatial medium (vacuum) just as traditional domains have their own mediums (solid, liquid, gas) (Dolman, 2022).

Table 1.1 therefore helps qualify aspects of disagreement about whether the human body can be a warfighting domain. If the domain concept does not require domain-specific movement, then the human body can be a warfighting domain in that it exhibits at least half of the remaining domain characteristics. The domain characteristics exhibited by the human body include specific modes of attack (e.g., pathogens, hacking IoB devices) that do not apply to other domains specifically. Furthermore, there are historical examples of weaponizing the human body in warfighting, such as medieval tactics that used infected persons to spread disease among besieged castles and cities (Wheelis, 2002).

This contrast with *space*, as a domain dominated by satellites and other unmanned craft, highlights another intersection of traditional domains with the human body as a domain; specifically, that traditional warfare on land, at sea, or in the air is focused on the destruction of human bodies. This begs the question of whether the human body is a domain of war distinct from the taking of human life during land, sea, or air domain operations. Medieval use of infections during sieges may be considered rightly as simply a form of bioweapon deployed strategically within the land domain. Thus, it is perhaps contingent on the ongoing development of biotechnology and the greater ability to leverage biocapabilities independent of conflict in traditional domains that will cause the human body to emerge increasingly as a distinct domain of warfighting.

China has made exploiting advancements in biotechnology and genetic engineering a high priority—especially for enhancing warfare and national defense—because its military leaders consider biotechnology the next revolution in military affairs. A significant amount of this research is conducted in military hospitals, especially the People's Liberation Army General Hospital. China's Academy of Military Medical Sciences, the National University for Defense Technology, and the Central Military Committee's Science and Technology Commission have made significant investments in "biology-enabled warfare" (Kania, 2019), which includes BCIs, brain networking, advanced biometric systems, human performance enhancements, and genetic engineering.

Chinese military leaders have also indicated that they consider biotechnology as among the new "strategic commanding heights" and are considering it a new military domain (Kania, 2019). Chinese military texts discuss offensive and defensive approaches to the biological domain, including dominance and deterrence through "ethnic-specific genetic weapons" (Kania and Vorndick, 2019). Regardless of what U.S. academics and strategists conclude on this definitional matter, that Chinese military leaders consider the human body to be a warfighting domain underscores the importance of our research.

Given this analysis, throughout the rest of this report, we adopt a halfway stance as to the degree to which the human body is a warfighting domain and will refer to our object of inquiry collectively as *human domain biotech*.

Chapter 2

Trends in Human Domain Biotech Development

Our team set out to explore the kinds of biotechnology applications that are in practice and that can plausibly be considered for the near future in a warfighting context. We then considered the risks and benefits of such technologies should they be integrated into defense strategies by the United States, its allies, and its adversaries.

Methods and Limitations

We identified three aspects of biotechnology—engineered pathogens, IoB technologies, and genomics—that collectively comprise what we refer to as human domain biotech and whose further development could substantially influence warfighting. These areas overlap significantly with the field of synthetic biology (Zegart, 2022). Given the broad scope of synthetic biology, we limited our insights to the three aspects of biotechnology discussed here.

Our research team met with other RAND Corporation subject-matter experts about each of the three aspects of human domain biotech. These discussions provided qualitative input that guided the team to available quantitative databases that were pertinent to each aspect, described in subsequent sections.

A necessary limitation of our research approach is that the results are exploratory in nature. They are not conclusive, and given the goal of quantifying innovation, they should be regarded as informed projections. In particular, an assumption of our research is that the pace of progress in these technologies will continue at a similar rate as it has in the past two decades. Another limitation is that this work does not consider other biotechnologies that might affect warfighters indirectly. For example, the potential consequences of adversary progress in the bioeconomy holistically—including (1) synthetic biology technologies related to agriculture and alternative energy sources and (2) genome-adjacent technologies, such as the microbiome or RNA modification—may affect national security and grand strategy considerations but are out of the scope of analysis for this report. Moreover, we limited our research to open-source information. We hope the results motivate further research and analysis of human domain biotech so that free states can work together to ensure a safe and prosperous world, even as humanity's technological powers over human bodies increase.

Engineered Pathogens

We compiled data from published sources on country-level cultural values known to enable strong societal resistance to pandemics and compared these data with records of the numbers of biosafety level 3 (BSL-3)[3] laboratories in these countries. Traditional analysis has long been concerned with the possibility of a state or nonstate actor using an engineered bioweapon (Department of Homeland Security, 2023; Mauroni, 2022). Bioweapons can be classified as either person-to-person transmissible or not transmissible (Department of Homeland Security, 2023; Global Biolabs, undated; Goad, 2021; Koblentz et al., 2023; Mauroni, 2022; Peters, 2018). In this report, we focus on the potential for transmissible bioweapon use because this use is most relevant for strategic actors, such as nation-states. This is because, in comparison with nontransmissible pathogens, transmissible ones (1) are inherently difficult to attribute to an actor or even to natural versus human causes (as we have seen with COVID-19), (2) have much greater potential for mass casualties and societal disruption, and (3) avoid the need for a mechanism to broadly disperse the pathogen, which is an inherent technical problem for nontransmissible bioweapons.

Nontransmissible bioweapons, such as aerosolized anthrax, might be strategically rational for a nonstate terrorist actor because they are much more attributable—aerosolized anthrax cannot infest the New York City subway system as an accident of nature. Terrorists usually want to take credit for their atrocities because this is how they seek to coerce political or other concessions. In contrast, it would be difficult for a terrorist group to prove that it, in fact, was responsible for a novel transmissible bioweapon, even if the group tried to prove it, because transmission via natural origins (such as zoonosis) is commonplace among transmissible pathogens. In fact, the only documented use of a bioweapon by a nonstate actor on U.S. soil was the salmonella poisoning by members of the Rajneeshee cult in 1984 in Oregon. Their goal was not biological terrorism (i.e., seeking to gain notoriety through horrific acts) but instead to sicken voters in particular precincts during a local election so that their own candidate would succeed. Although their electoral ambitions failed, the case highlights how bioweapons could be used strategically by a nation-state because the Rajneeshees' salmonella outbreak was mistaken as a natural occurrence, and only after more than a year of investigation was the plot ascertained (Parachini and Gunaratna, 2022). These same authors note that both al-Qaeda and the Islamic State examined bioweapons for the purpose of biological terrorism, but they did not pursue bioweapons because other means of terrorism (bombs, guns, planes) were so much more available, attributable, and easier to deploy.

Past natural zoonotic diseases have taken decades of research to fully establish their origins through epidemiology and evolutionary genetic investigations. This is the case with the most deadly zoonosis of the 20th century, HIV, whose exact origin still is debated; some contend that needle reuse during mid–20th century vaccination campaigns against African sleeping sickness might have

[3] A *BSL-3* or a *Pathogen (P)3 lab* is a research laboratory with biocontainment facilities that conform to worldwide requirements for handling pathogenic microorganisms that are airborne or whose toxic properties are transmitted by air. Laboratories are classified into four BSLs based on the pathogenicity of the agents handled in them. For example, BSL-1 laboratories handle low-risk microbes, such as nonpathogenic strains of *E. coli*, and BSL-2 laboratories handle such agents as human immunodeficiency virus (HIV) that are not transmissible through casual contact. In contrast, SARS-CoV-1 and -2 and influenza can be handled only in BSL-3 or BSL-4 laboratories because they both cause illness *and* are highly transmissible through the air, while the Ebola virus is a BSL-4 agent because of its high lethality.

exacerbated HIV's spread through Africa after an initial zoonotic transfer via bushmeat butchering (Carlsen, 2001; Gürtler and Eberle, 2017). The intrinsic ambiguity of disease transmission is a strategic asset for actors who wish to achieve concrete goals (e.g., rigging an election, depleting force effectiveness in advance of kinetic strikes) in a clandestine manner. Conceivably, disease transmission mechanisms could be tailored to target populations or groups that engage in particular behaviors that facilitate a particular transmission mode. For example, eating uncooked vegetables or meat makes a person vulnerable to particular foodborne illnesses that are much less likely without these behaviors, and patterns of sexual partner-switching are intrinsically related to the epidemiology of sexually transmitted infections.

That said, we cannot rule out the possibility of a strategic or irrational nonstate actor who simply wants to spread mayhem and death regardless of whether they can take credit for their actions. But this would seem a low-probability concern because empirical research and conventional logic establish that terrorists want to take credit for their actions (Matthews, 2020).

These features of transmissible bioweapons make such weapons strategically rational for certain nation-state armed conflict scenarios. Nation-states would seek to use bioweapons in coordination with other modes of warfare—e.g., warfare in the land, sea, or air domains—to accomplish operational objectives. Lack of attribution is a desirable property in this context because nation-states most likely will not use these weapons to coerce concessions; they will use them to degrade military and supply-chain capabilities to accomplish traditional nation-state objectives, such as seizing territory and controlling populations.

The easiest technical means for realizing a transmissible bioweapon would be for a malicious actor to gain access to a laboratory already equipped to manipulate high-risk pathogens. While a malicious actor could develop a bioweapon by independently acquiring all the needed materials, potentially via a do-it-yourself (DIY) biology model (Kolodziejczyk, 2017), a likely easier path to achieving this aim would be to access an existing BSL-3 laboratory.

Monitoring and policing every individual's intentions is an impossible task, so a key defense against the use of a bioweapon by a nonstate actor is to reduce the overall access to BSL-3 or -4 facilities. This can be accomplished through vetting of personnel, but inevitably such vetting must have a nonzero failure rate. Thus, another important proposed safety measure is simply to reduce the ongoing proliferation of BSL-3 and -4 facilities. This can be a defense against nonstate malicious actors and against wholly unintentional accidents in which pathogens "leak" out of a lab by infecting lab workers who then pass the infection onto others. China experienced two documented leaks of SARS-CoV-1 from its labs prior to the COVID-19 pandemic (Enserink and Du, 2004; Walgate, 2004), and these SARS-CoV-1 leaks were part of the impetus for some academic researchers to call for regulations that would restrain the still ongoing proliferation of labs that handle dangerous pathogens capable of pandemic spread (Klotz and Sylvester, 2014; Merler et al., 2013). Assuming only *accidental* risk, Klotz and Sylvester (2014) stated, "there is a substantial probability that a pandemic with over 100-million fatalities could be seeded from an undetected lab-acquired infection," and this probability can only increase if we add the potential for malicious actors to access labs to the list of risks.

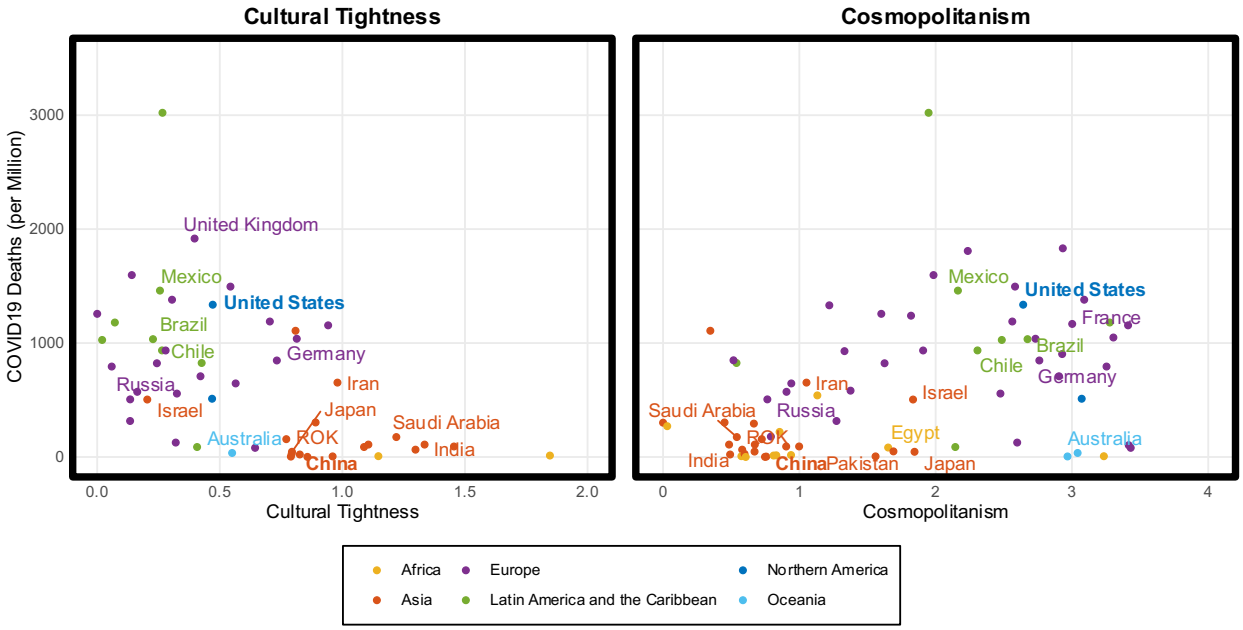
The main international regulation for dangerous pathogens is the Bioweapons Convention (BWC). Although 185 countries are signatories to the BWC and thereby have pledged not to develop

biological agents for warfare, the BWC makes no restrictions on the number of BSL-3 and -4 laboratories that a country may have, nor does it facilitate or require any formal registry or other record-keeping for these facilities (Biological Weapons Convention, 1976).

We consulted several existing databases compiled by academics, including one that was the most comprehensive (Peters, 2018), to assess the number of BSL-3 laboratories. We focused on BSL-3 because most BSL-4 pathogens, such as the Ebola and Marburg viruses, are so lethal that they are unlikely to cause major disruption to the U.S. military or U.S. society more generally. This assessment is based on experience, which has shown that the U.S. public health system's epidemiological protocols—which focus primarily on diagnosis, isolation, treatment, and contact tracing—have been highly effective in preventing community spread of Ebola (van Beneden et al., 2016).

This medicalized approach to pandemic control proved less effective to control the spread of COVID-19. The spread of COVID-19 was a result of its much lower mortality rate post-infection (referred to as case fatality rate [CFR]) and substantial level of asymptomatic spread compared with Ebola, which enabled infected people to move about and spread the pathogen, all largely unwittingly. These factors also rendered contact tracing ineffective and inefficient as a countermeasure. Societies that did best against COVID-19 were those that were able to spur nearly their entire population to adopt simple behavioral rules (such as masking or avoiding large groups) that reduced the spread of the pathogen in aggregate. This aggregate reduction prevented cases and thereby prevented overall mortality, even if it did not reduce CFR (Figure 2.1). Certain cultural values that show long-standing differences among countries were the most important predictors of a country's ability to mobilize the population *en masse* to adopt behavioral COVID-19 mitigation measures: These are cultural tightness and cosmopolitanism (Gelfand et al., 2021; Ruck, Borycz, and Bentley, 2021; Ruck et al., 2020). Ultimately, the COVID-19 pandemic ended in a state of global SARS-CoV-2 endemicity: Infection levels were brought into a steady state by population immunity, and that was achieved either through natural infection or vaccination. As with nonpharmaceutical infection control measures, compliance with vaccination fundamentally is a choice heavily influenced by cultural factors (Matthews et al., 2022).

Figure 2.1. Long-Standing Differences in Cultural Values Affected COVID-19 Mortality



SOURCES: Features information on cultural tightness from Gelfand et al., 2021; cosmopolitanism from Ruck et al., 2021; and COVID-19 deaths from Mathieu et al., 2020.

Cultural tightness is a measure of a society's emphasis on following rules simply because they are rules, while *cosmopolitanism* is a measure of a society's willingness to tolerate those who violate social norms and expectations. While these measures are correlated, they are distinct conceptually and empirically, and the studies whose findings are shown in the left-hand and right-hand panels of Figure 2.1 were conducted independently and used different survey data sources. All this points to these patterns being scientifically robust and likely to repeat in the next pandemic. We note that some of these values are things that, for other reasons, Americans do not and should not want to change. In other research, we have shown that, in particular, cosmopolitanism is among the best predictors of whether or not a society is a democracy or autocracy; it even predicts democratization 20 to 30 years in advance of governmental institutions forming (Ruck et al., 2020). This is because a willingness to tolerate immigrants; people of other races; or those with different languages, religions, or lifestyles is what is required to be a liberal democracy: A truly open society fosters that type of diversity. If the majority of participants in a society are not willing to tolerate such diversity, then they do not want to do what being a democracy requires, and democracy predictably fails under these cultural conditions.

Because the United States cannot change its relatively cosmopolitan culture, it can expect to be relatively disadvantaged in a global release of a BSL-3 bioweapon. While our opening scenario (Vignette 1) focused on the potential for China to use a bioweapon to achieve a near-term and spatially discrete objective, China would also be on the advantaged side of a more global release.

More-speculative scenarios could be imagined for a state actor seeking to create a disruption similar to what we witnessed during COVID-19, particularly in the democratic West, which tends to have cultural values that preclude robust BSL-3 disease mitigation by their populations (for an

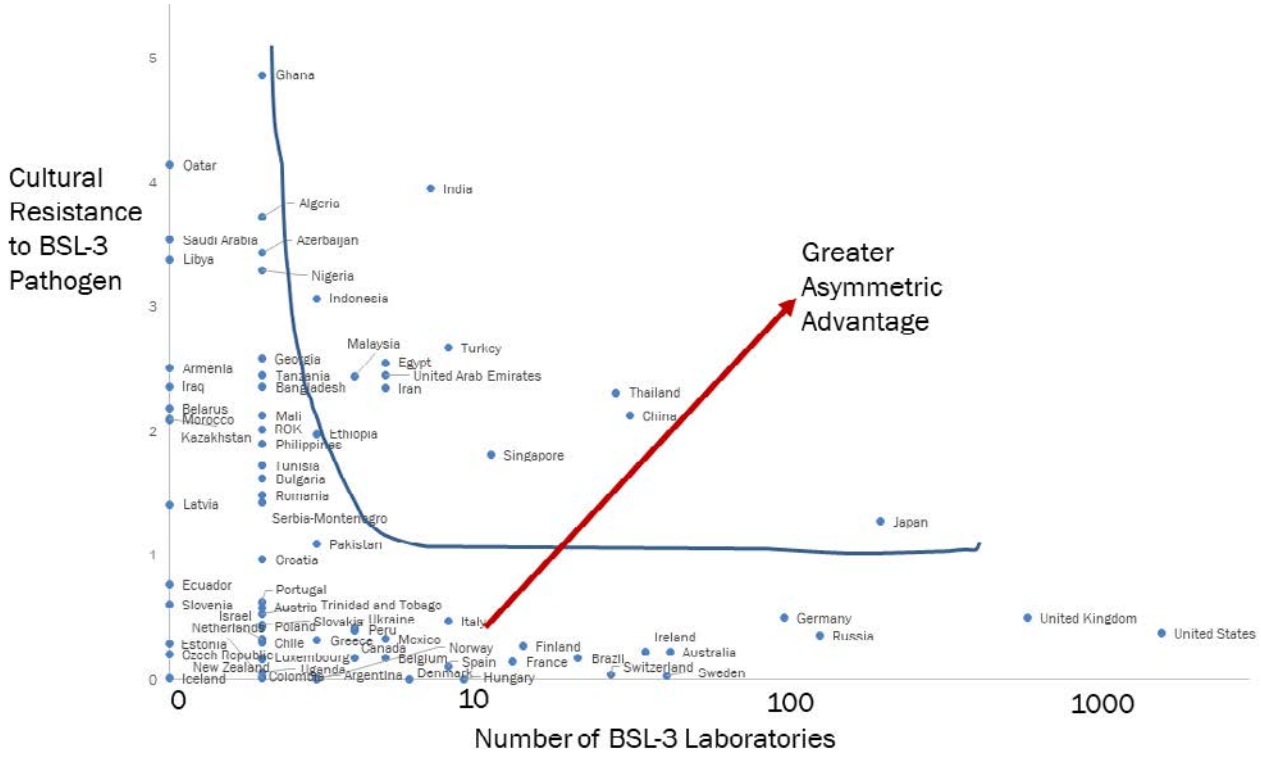
example of such a scenario, see Vignette 2). This scenario could be coordinated as part of a propaganda, military, and economic campaign to produce a tipping point away from the existing world order to reshape it into a set of economic and alliance connections that center on a cadre of autocratic states. Countries that exhibit cultural advantages in this type of scenario, and the capability to engineer pathogens in BSL-3 facilities, are shown in Figure 2.2.

Vignette 2. Pandemic Geopolitics

It is a seasonably hot and sticky summer in Washington, D.C., in August 2033 when a novel airborne pathogen begins spreading. Public health officials scramble to improve ventilation and filter compliance for air-conditioned spaces—features that had long since lapsed into deregulation and disregard since the COVID-19 pandemic. The new infection exhibits an astonishingly long asymptomatic contagious period of three weeks, followed by a 2.5-percent mortality rate. Contact tracing fails as an intervention because of the amount of asymptomatic spread, and by four months after the infection was first detected, nearly 1 million Americans are dead. With a projected 6.5 million still to die, essential workers reasonably insist on reduced person-to-person contact until a vaccine is produced. U.S. and Western European supply chains reduce to one-third of their original throughput.

China and Russia, meanwhile, are relatively unaffected by the virus because they had advance access to an effective vaccine. China readily deployed the vaccine to its now even more ethnically homogenous and compliant population, while Russia used brutal crackdowns against anti-vaccine populists. As Russia and China launch simultaneous aggressive moves on their borders, the United States and its European allies are unable to muster public will to mount a unified resistance. Regardless, their military supply chains are interlinked with civilian ones, severely compromising any military response had they raised one. Several former Soviet countries are annexed wholesale into Russia. Other nearby countries, e.g., India, sign stringent treaties with the aggressors to retain sovereignty. The Pax Americana, fraying since the invasion of Ukraine in 2022 and annexation of Taiwan by China in 2028, is officially ended.

Figure 2.2. Country-Level Cultural Resistance to BSL-3 Pathogens Versus Capabilities for Production



SOURCES: Y-axis from study team calculations. Cultural resistance to BSL-3 pathogen calculated as the product of tightness and cosmopolitanism after each standardized to a 0–5 Likert-type scale. BSL-3 counts are derived from Peters, 2018.

While China and Russia feature in the scenario of Vignette 2, undeniably, global geopolitical tensions could be very different ten years from this writing. However, such researchers as Gelfand et al. (2021) and Ruck, Borycz, and Bentley (2021) have shown that the cultural values that are among the most predictive for pathogen mitigation are multigenerational patterns that are highly resistant to change. Figure 2.2 identifies the countries that we can predictably anticipate will be on the relatively advantaged side of an airborne pathogen pandemic, and these patterns will persist ten and even 20 years from this writing.

Internet of Bodies

The IoB includes such devices as fitness trackers, wearables, and other smart consumer devices, as well as such internet-connected medical devices as pacemakers, exoskeletons, and prosthetic limbs. Advanced IoB devices, such as smart contact lenses, are also under development (Jin et al., 2023). Matwyshyn (2019) characterizes the IoB as a progression of the Internet of Things and defines the IoB in three generations: body external, body internal, and body melded. Such technologies have the potential to transform warfighting.

IoB and related technologies present a variety of potential opportunities to warfighters. For example, the U.S. Army is running studies to determine whether wearables can help with soldier well-

being and fitness (Fish, 2023). Australian researchers have shown that military robot quadrupeds can be steered by brain signals collected and translated by a graphene sensor worn behind the ear of a nearby soldier (Tucker, 2023). In May 2023, the U.S. Space Force (USSF) announced plans for a large study in which guardians can choose between using wearable devices and participation in the traditional annual physical fitness tests to assess physical fitness (Hadley, 2023).[4] This plan can help USSF track fitness continuously and focus on year-round health rather than driving its personnel to engage in dangerous habits, such as eating disorders, in the months leading up to annual body weight checks and fitness tests (Schmid, 2022).

Combining IoB data with advanced machine learning (ML) and AI algorithms can potentially enable tremendous advancements in health care, particularly precision medicine. AI has opened the door for more-efficient and automated analysis of complex data from across diverse sources. These algorithms speed up the data pipelines that are often necessary to support the complex interaction of human-machine interface. The collection and analysis of data collected on human physiology, activity, and genetics require efficient algorithms to manifest practical results (Hinkel, 2022). AI/ML algorithms can be trained on the vast amount of data collected by the network of IoB devices and predict acute or chronic changes in health status. For example, DoD is investing in wearable technologies using AI algorithms that could predict infection up to 48 hours before symptoms appear (Vergun, 2023).

Although IoB technologies offer significant potential and have already realized benefits, some have also been shown to incur risks to the warfighter and to national security. One type of IoB risk derives from information security issues with IoB-collected data. In early 2018, it was discovered that the publication of a heatmap of users' running routes by the fitness app Strava revealed sensitive location and layout information of U.S. military bases around the world (Hsu, 2018). A security vulnerability in the Strava app reportedly allowed unknown users to identify and track the movements of Israeli service members inside military bases, even if users limited who could view their Strava profiles (Brown, 2022; Hern, 2022). In 2023, it was reported that the Strava app might have been used to track a Russian submarine commander who was killed while jogging (Knight et al., 2023). In response to the first Strava incident, in August 2018, DoD banned personnel from using apps with geolocators while in overseas operational areas (Browne, 2018). However, these devices are in wide use outside military operational contexts. We present a scenario in Vignette 3 in which an insider threat uses an IoB device to capture sensitive government data.

[4] *Guardian* is the term used to signify a space professional working in the USSF (Secretary of Air Force Public Affairs, 2020), analogous to an Army soldier or Navy sailor.

Vignette 3. An Insider Threat Uses the Internet of Bodies to Steal Sensitive Government Information

In 2027, a mid-level U.S. government employee undergoes cataract surgery in one eye, during which the natural lens inside the eye is replaced with an artificial lens to restore vision. The surgery, which takes about 15 minutes, is extremely safe and is performed on millions of people a year.

One big difference, though, is that this new lens contains a tiny camera, which is connected to a micro storage device placed subcutaneously at the man's temple and hidden under the hairline. This allows him to capture and store images of everything he sees.

The employee has access to highly restricted government facilities and sensitive documents. As soon as he has healed from the surgery, he begins a months-long effort to collect as much information as he can about U.S. military plans and intelligence activities. He sends this information back to his home country, which pays him a handsome sum. The U.S. government is unaware of the leaked information and is unable to understand why its military operations are unsuccessful.

One IoB technology—BCIs—may have a particular impact on warfighting. BCIs collect electrical signals from the brain and translate them into external outputs, such as commands (Shih, Krusienski, and Wolpaw, 2012). BCIs can be body external (e.g., a noninvasive electroencephalogram [EEG] wearable cap) or body internal (e.g., implanted into the brain). Some BCI technologies have shown promise for people who have lost the function of certain limbs or neuromuscular capabilities by *reading* brain signals (Ouellette, 2022). A fighter pilot who has lost function of their limbs could thus potentially use this technology to connect to and operate an aircraft. Future BCIs might even have the ability to *write* to the brain (Binnendijk, Marler, and Bartels, 2020). A military commander could use this technology to communicate with their forces about a change in commander intent or a pivot in battlefield tactics. But if this technology were hacked, a malicious adversary could potentially inject fear, confusion, or anger into the commander's brain and cause them to make decisions that result in serious harm. In fact, several organizations based in China were found to "use biotechnology processes to support Chinese military end uses and end users, to include purported brain-control weaponry" (Department of Commerce, 2021), and, because of this, these entities were added to the Department of Commerce's Entity List to restrict trade with those organizations. In Vignette 4, we present a hypothetical scenario in which BCIs gravely challenge national security.

Vignette 4. Brain-Computer Interface That Influences Mood

In 2050, a few octogenarian congressional leaders face tough re-election campaigns because of rumors of ill health and poor cognitive fitness for their roles. Three of these members of Congress quietly have state-of-the-art BCIs implanted into their brains, a practice that has become somewhat commonplace among wealthy senior citizens. The members had previously shown signs of slowing down, but this BCI enables them to move and speak normally, particularly with the help of political allies who conceal their true condition.

The BCI developers suspect that their implants have the ability not just to read brain signals but to affect the users' temperament in subtle and inconspicuous ways. However, the developers keep this quiet because they have not been able to identify a fix. This susceptibility in the BCI ends up causing much confusion for the congressional leaders in this scenario. They have episodes of erratic behavior, forgetfulness, and irrationality, and they take a belligerent approach with their fellow members of Congress, allies, and partners. The U.S. populace is demoralized. Once-friendly countries begin to distance themselves from the United States.

To characterize emerging IoB technologies relevant to the warfighter, we investigated the cumulative number of patent applications filed in a variety of IoB technology areas.[5] We looked for what we refer to as *technology emergence*, the rapid growth over time of the cumulative number of patent applications that were assigned by patent examiners to a specific technology subclassification. This is an indication that many individuals or organizations were submitting applications in the same specific technology area in a particular period. Technology emergences are time-dependent and typically follow a logistic or S-curve, representing diffusion of the emerging technology through a technological network, and can be inferred from co-assignments by patent examiners of the same technology to different subclassifications in the technical hierarchy of the patent-granting organization (Eusebi and Silberglitt, 2014).

For this effort, we used patent data from the IFI claims direct platform. This dataset includes full-text patent data from 38 countries, as well as metadata, such as filing date, patent classes, assignees, and drawings. The data include more than 100 sources and 125 million records. Patent text is machine-translated to English, and its format is standardized to facilitate analysis (IFI Claims Patient Services, undated).

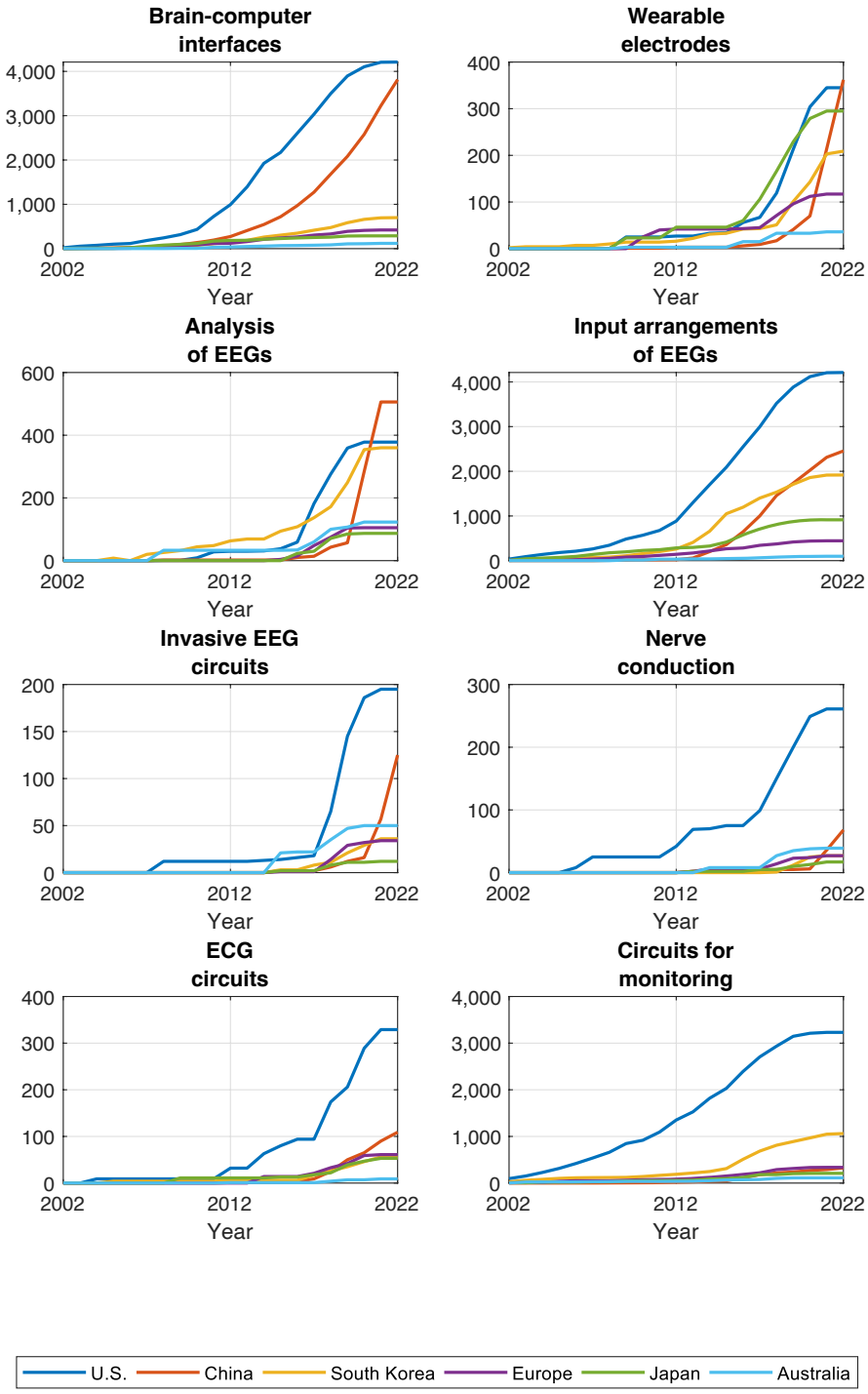
The analysis of patent applications presented here was limited to technologies related to BCIs, monitoring technologies, and wearable electrodes. The data show that the United States has a lead of about three to five years in many of the patent application categories that we evaluated, such as input arrangements of EEGs, invasive EEG circuits, and nerve conduction (see Figure 2.3). However, in the case of wearable electrodes and analysis of EEGs, China's patent applications surpassed those of the United States in 2021 and 2022, and, in the case of BCIs, China is quickly catching up. If the trends continue as expected, China likely will catch up to the United States in IoB human domain biotech areas within the next few years.

We acknowledge limitations to this analysis. Patent applications do not necessarily indicate dominance in a particular technology area, they may not result in patents granted or in the adoption of such technologies, and military operational benefits of such devices may not materialize. This analysis

[5] These technology areas are defined by classifications and subclassifications in a technical hierarchy established by national and international patent-granting organizations. For this work, we used the Cooperative Patent Classification scheme from the U.S. Patent and Trademark Office, undated.

provides only a limited overview of trends in a narrow range of IoB technologies. Nevertheless, these patterns are an indicator of the extent to which China is investing in these technologies; moreover, previous work discusses China's activity in a cluster of related areas of biotechnology (Blumenthal et al., 2021). These trends suggest that the United States might be losing its advantage in this space.

Figure 2.3. Trends in Patent Applications of Internet of Bodies Technologies



SOURCE: Features information from IFI Claims Patient Services, undated.
NOTE: ECG = electrocardiogram. In this figure, patent application counts were limited to technologies related to BCIs and wearable devices.

Genomics

Similar to other emergent scientific fields, *human genomics*—the study of humanity's genetic makeup—holds substantial transformative promise, potentially altering humanity's relationship with nature in ways that can be both beneficial and costly. Human genomics has profound implications for the present and future of human warfighting. Genomic knowledge may revolutionize how militaries prepare and equip their soldiers, enhancing their resilience and optimizing their performance and recovery. From personalized (precision) nutrition and training regimens to advanced medical treatments and even genetic enhancements, genomics could provide the key to supporting a new generation of warriors who are better equipped to overcome the vicissitudes of modern warfare.

For the most-speculative area of genomics, we conducted a systematic quantification of publications in genomic technologies by authors' countries as a way to identify growth and innovation. We found two typologies—*surveillance* and *enhancement*—within the context of genomic science applications to warfighting:

- **Genomic surveillance** combines genomic data with sorting, identifying, and surveillance technologies.
- **Genomic enhancement** is the process of isolating and using accessible genomic information or treatments to alter a trait in the human body or the environment to enhance resiliency at a micro (individual) or macro (societal) scale.

These typologies represent a conceptual framework for evaluating possible use cases when genomic technologies interact with a warfighting environment. This is not an exhaustive or comprehensive list of typologies; rather, these represent what we believe to be the most-relevant applications within the concept of the human body as a warfighting domain.

Genomic Surveillance

Genomic surveillance is a near-term capability already in use in the private sector and deployed by other countries to identify genomic patterns. These technologies are used to analyze ancestry, track viral mutations within human cells, and survey microbial evolution within the environment (CDC, 2023). The biggest challenge to applying genomic surveillance to warfighting forces is to find robust correlations of genotypes with characteristics (phenotypes) that effectively align with military roles. The most prominent technique for finding such genotype-phenotype associations has been the use of genome-wide association studies (GWAS), but GWAS may have plateaued in their ability to find meaningful associations due to the complexity of the human genome (Singh and Gupta, 2020). For over a decade, researchers have proposed that advances in AI will produce a robust understanding of genome-phenome links, but this has yet to materialize (Computational Pan-Genomics Consortium, 2018). Writing in *American Scientist*, de los Campos and Gianola (2023) contended that new AI algorithms are unlikely to surpass insights from GWAS anytime soon because vast genomic complexity and relatively small sample sizes that can realistically be achieved for humans mean that AI will be unable to solve the task at hand. Essentially, because genomic complexity is so vast, it may take

training samples in the tens of millions for AI to actually solve gene-gene and gene-environment interactions in a way that GWAS cannot.

This seems counterintuitive because large language models (LLMs) have shown such great success at replicating human language, but language has an important contrast with genomes in that the former is intrinsically a system of meaning created by intelligent agents (humans). LLMs are AI that is replicating natural intelligence. Meaningless utterances are rare. Thus, the training data for human language are many orders of magnitude more richly informative (low noise-to-signal ratio) than are genomic data. Genomes also are information systems, but they are created by a wholly unintelligent algorithm—Darwinian evolution—that, although it produces beautifully adapted creatures, it does so through an immensely inefficient and even wasteful process. Evolutionary biologist and science communicator Richard Dawkins famously riffed off the theologian William Paley and called evolution a "blind watchmaker" (Dawkins, 1986), but in contrast with LLMs and language, the evolved genome can aptly be called a "tale told by an idiot" (*Macbeth*).

Should the challenges of genome-phenome associations be solved in the near future, then genomic data may be useful to identify traits in warfighting forces that could be used in a predictive sorting model. For example, if a nation-state needed to employ a military draft and the relevant genomic and phenotypic data were adequately collected and stored, then a learning algorithm might sort candidates into the proper class of job for the term of service or perhaps develop a hierarchy of associated jobs using demand. These data, properly collected, can be crosswalked with other data sources to identify key traits for recruitment. In Vignette 5, a short narrative highlights how a combination of genomic data could support the selection of military recruits. Genomic surveillance will only be a value-add, however, if it predicts potential or future phenotypic traits that are not easily observable through phenotype itself. For example, a genetic test that predicted height or strength would seem relatively useless because these features are more easily and inexpensively observed in the phenotype directly. In contrast, a genetic test that predicted the potential for an individual to master a specialized BCI after weeks or months of training might be highly valuable if this future potential were not readily observable phenotypically.

Vignette 5. Genomic Recruitment Screening

In a recruiting office, a taciturn USSF captain supervises the 343 incoming recruits assigned to participate in a new orbital drop trooper program. The captain quickly reviews the selection data on their tablet. Each candidate has several composites of ability scores with detailed genomic histories. The genomic data gathered during Selective Service registration allows the rapid identification of candidates for several special programs using genetic potential. An evaluation by a think tank had shown that the U.S. Air Force (USAF) had improved the efficiency of pilot selection by 15 percent through the application of genomic tools. The USSF's orbital drop trooper program was different and far more demanding than the USAF pilot selection program; each candidate would be expected to endure the tribulations of high-altitude jumps, such as Felix Baumgartner's historic 127,852-foot jump. The captain knew this program was experimental and risky; thus, only those who met the stringent standards could be recruited.

Genomic Enhancements

The most future-focused of our typologies is genomic enhancement—the ability to temporarily or permanently enhance an individual's genomic traits. Genomic enhancement has been the stuff of science fiction and comic books for many decades. The desire to create supersoldiers has deep historical roots in early experimentations, starting as far back as the late 19th century (Lin et al., 2014). Much of *eugenics*—the attempt to use reproduction to increase the proportion of individuals with desirable traits—derives from a fundamental misunderstanding of human genomics and a desire to enhance genetic traits in fighting forces (Roll-Hansen, 2010). These pseudoscience theories contributed to the justification of ethnic cleansing and the rise of genocide later in the 20th century (Bashford and Levine, 2010).

The development of genomic enhancement and its role as a technology application have been much discussed in literature. Potential near-future genomic enhancements of key warfighting traits could be the ability to function with less sleep, more physical stamina, and improved breathing capacity (Almeida and Diogo, 2019; Blendon, Gorski, and Benson, 2016; National Academies of Sciences, Engineering, and Medicine, 2017). Genomic enhancement as an actionable tool is early in its scientific understanding and development. Deploying genomic enhancement has several limitations, many of which are associated with scalability, sequencing time, and cost. Although sequencing time and cost have decreased by over six orders of magnitude since 2000 (National Human Genome Research Institute, 2021), it remains to be seen, as noted previously, how well genetic sequences can be interpreted meaningfully with respect to a person's traits, and how well synthetic biology enhancement tools will scale in the future. It is unlikely that genomic enhancement of the warfighter will be realistic within the next five years, when scientists can only just now—20 years after the Human Genome Project (HGP), whose goal was to sequence the whole human genome—cure single-locus diseases, such as sickle cell anemia.

Given the aforementioned constraints for the warfighter, genomic enhancement might be applied soonest to highly specialized missions in which a marginal positive change in some physical or psychological activity would tip the balance toward benefit. In Vignette 6, we present a vignette that explores a far-future application of genomic enhancement.

Vignette 6. Genomic Enhancement for Degraded Environments

By 2050, the National Aeronautics and Space Administration's Artemis program has been a great success for over two decades, enabling astronauts to conduct a variety of missions to explore the lunar surface. However, with the establishment of a few permanent Moon bases, a new Cold War has broken out among the major spacefaring countries because of competition over ownership of those bases. The USSF sends a plucky young captain on her first support mission to the Moon. As the spacecraft hurtles toward one such contested base, she gazes out the window at the moonrise.

Moments before landing, a breach in the carbon fiber shell of the captain's spacecraft—a breach likely caused by this trip being the ship's fifth reuse—has caused the craft to veer off course. The captain lands miles from the Moon base without the air and water levels needed to make it by rover. The captain calls back to her home station and requests support. The operations center commander informs the captain that she has been authorized for the emergency use of genomics enhancement for degraded environments, which should slow the captain's breathing and water consumption and extend her life support by 96 hours. The captain stops voice communications to preserve her oxygen and water supply. Those 96 hours allow just enough time for another spacecraft to be launched with resupply materials, and, after a flurry of transmissions, the captain confirms that she survived.

Genomic Technologies in the Age of International Competition

Genomic research is a key strategic asset for national security, but its complexity creates deep uncertainty in when or whether genomic advancements will be truly useful to the warfighter. Nevertheless, China has been conducting applied gene research for potential military use. One example is a prenatal genetic test developed by BGI Group, formerly known as the Beijing Genomics Institute (Needham and Baldwin, 2021). In 2021, it was reported that BGI worked with the Chinese military to help increase "population quality" using the data gathered from this prenatal test (Needham and Baldwin, 2021).

Understanding the landscape of genomics research is critical to understanding global competition in this area. We examined recent (within the past ten years) genomic publications, using data from the Web of Science, to track the progress of genomic-focused research, and found that the United States and China are leading the way and are neck-and-neck in overall publications.

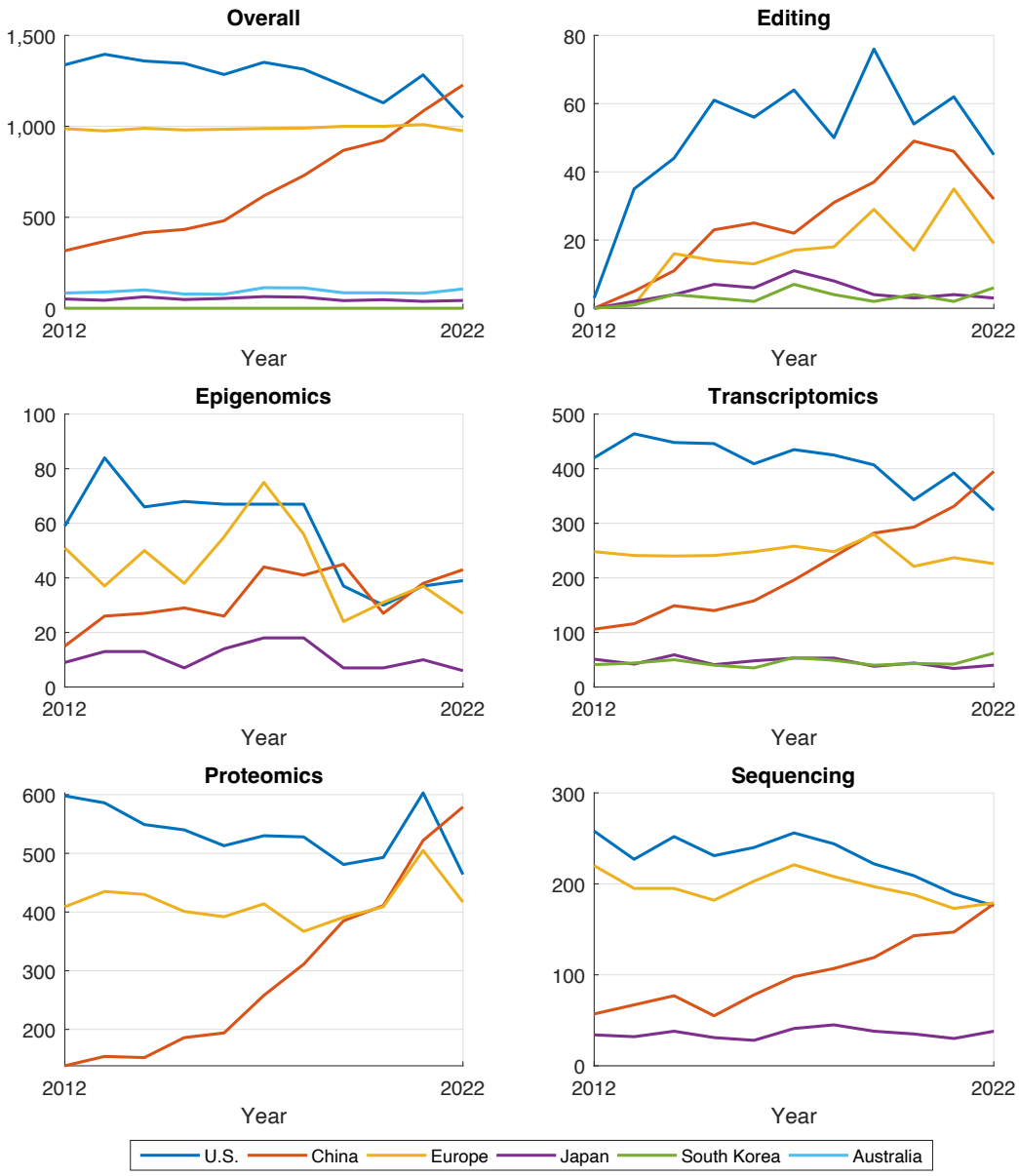
To understand these trends better, we segmented the publication dataset into five categories of genomics research. These categories represent five key technology areas that enable the warfighting genomic typologies of surveillance and enhancement that we described previously:

1. *Genomic editing*: Also called *gene editing*, this is an area of research seeking to modify genes of living organisms to improve our understanding of gene function and develop ways to treat genetic or acquired diseases (Committee on Human Gene Editing, 2017).
2. *Epigenomics*: This is a field of study, also sometimes called *epigenetics*, that is focused on changes in DNA (deoxyribonucleic acid) structure that do not involve alterations to the underlying gene sequence (National Human Genome Research Institute, 2023b).
3. *Transcriptomics*: The DNA sequence of genes carries the instructions, or code, for building proteins. As the first step, a gene is transcribed into a related molecule, mRNA. The transcriptome is a collection of all the mRNA molecules (gene readouts) present in a cell, at any given time (National Human Genome Research Institute, 2020).

4. *Proteomics*: The mRNA molecules serve as intermediate templates that are then translated into proteins; proteomics characterizes the total and individual pattern of proteins in a tissue or organ (National Human Genome Research Institute, 2018).
5. *Sequencing*: To sequence a person's DNA, researchers follow three major steps: (1) purify and copy the DNA, (2) read the sequence, and (3) compare it with other sequences (National Human Genome Research Institute, 2023a).

The clear pattern across all keyword groups in this analysis is that the United States has dominated in all areas of genomic research publications, but an emergent China shows an upward trend in publications that threatens to overtake those of the United States (Figure 2.4).

Figure 2.4. Genomic Citation Counts Across Country and Technology Category



SOURCE: Features information from Clarivate Analytics, undated.

This analysis has some limitations. The associated publication counts represent an incomplete heuristic of national knowledge; the genomic technology postures in other countries have many unknowns. One such unknown is that raw counts do not consider the quality of research. Additionally, the private market plays a large role in developing new technology, and the nature of counting reported research articles is tricky. Because of the deeply collaborative nature of genomic research, many other countries send their scholars to conduct research in—or simply collaborate with—U.S. universities and other research institutions. Furthermore, U.S. institutions have a culture

of "publish or perish" that may result in more-aggressive publication reporting. Finally, U.S. research institutions have diverse sources of funding that can support a wide and diverse genomic research field. Reported values simply represent overall trends and are not wholly complete. Nevertheless, these results demonstrate that China has been aggressive in expanding genomic research funding and opportunities for collaboration.

Chapter 3

Risks and Opportunities of Human Domain Biotech

Engineered pathogens, the IoB, and genomics are biotechnologies for the human domain that will continue to innovate in the next five to ten years and longer. Innovation in these areas may even accelerate compared with the time of this writing, although whether this happens and in what application areas is uncertain. Using the research summarized previously and discussions with subject-matter experts on these topics, we identified several notable risks and opportunities, presented across these biotechnology domains in Table 3.1.

Table 3.1. National Security Risks and Opportunities of Human Domain Biotechnology

	Biotechnology Domain		
	Engineered Pathogens	**Internet of Bodies**	**Genomics**
Risks	1. **Achieve near-term land grab by nation-state** 2. **Achieve long-term geopolitical reset by nation-state** 3. **Achieve societal chaos for nonstate actor**	1. **Siphon data to gather details about secret military installations** 2. **Obtain compromising personal information about important U.S. personnel** 3. *Hack IoB technologies like implanted BCIs*	1. **Identify minority groups for persecution** 2. *Enhance adversary soldiers* 3. *Design a pathogen to target U.S. populations* 4. *Raise genetically engineered supersoldiers from embryo*
Opportunities	Limited for the United States because it is likely to comply with the BWC and is on the disadvantaged side of cultural resistance to BSL-3 pathogens	1. **Detect pathogens** 2. **Replace lost capabilities (e.g., limbs, hearing)** 3. *Reduce physical training time* 4. *Augment existing capabilities*	1. *More quickly and efficiently screen soldiers into combat roles, especially in the context of mass mobilization* 2. *Genetic engineering to augment capabilities (e.g., altitude tolerance)*

NOTE: Bold items are likely realizable within five years of this writing. Italicized items are likely at least five or more years in the future.

As Table 3.1 shows, engineered pathogens present risks but almost no opportunities for the United States. This is because the United States very likely will continue to abide by its commitment

to the BWC, which prohibits the development of pathogens for biological warfare. But U.S. adversaries are unlikely to adhere to the BWC—the Department of State (2022) has published concerns about noncompliance with the BWC by China, Iran, North Korea, and Russia. In particular, use of a bioweapon to achieve an immediate land-grab goal could be a strategically rational option for several U.S. competitors and adversaries. Using bioweapons as part of a plan for broader geopolitical restructuring or as a plot by a nonstate actor to sow anarchy seem like less clearly rational calculations and are probably less likely.

Several IoB technologies are realizable today or likely in the very near future. The 2018 Strava incident is a small example of how use of IoB technologies could reveal critical information to U.S. adversaries. Risk of information compromises will only increase as more IoB technologies are deployed to a greater proportion of the U.S. population. Detecting pathogens and replacing lost or compromised capabilities through IoB have shown rapid advances in recent years (Ouellette, 2022; Vergun, 2023) and present opportunities for improved tactical performance and readiness for military units. Longer-term IoB developments are uncertain at this point. For example, it remains unclear whether BCIs will be truly tractable to enhance military operations under realistic field conditions. It is similarly unclear at the time of this writing whether IoB can truly enhance human physical performance or substantially reduce training times for physical or mental conditioning. Each of these possibilities presents risks and opportunities for the warfighter.

Because of the highly complex nature of genomic systems, genomic technologies bear mostly speculative risks and opportunities that are at least five years in the future: Genetic advancements have tended to happen in a two-steps-forward and one-step-backward fashion. The translation of the HGP into patient benefits remains a work in progress. On the cusp of the project's 20-year anniversary, Joyner and Paneth (2019) wrote,

> [N]early two decades after the first predictions of dramatic success, we find no impact of the Human Genome Project on the population's life expectancy or any other public health measure, notwithstanding the vast resources that have been directed at genomics."

This was essentially the same assessment of the clinical impacts of the HGP at ten years (Hall, 2020). Advancement in genomic technologies will rely on continuing progress in other biotechnology innovations, as well as in data science. Efforts, such as the All of Us Research Program by the National Institutes of Health, can help pave the way for radical improvements in genomics research (National Institutes of Health, undated).

In contrast with most genomic innovations in Table 3.1, genomic screening to ascertain an individual's identity or ancestry is an already well-characterized technology. This technology has been used successfully by law enforcement in the United States and globally, but in the future, it may carry risks to the safety of minority groups living under oppressive regimes (Wee and Mozur, 2021).

Recommendations

Our research suggests that U.S. policymakers should consider the following priority areas for action. We have divided them into near-term (within five years) and longer-term (five-plus years) recommendations. We note also that longer-term recommendations are much less certain because it is

much less known what will be technologically achievable more than five years from now. Some anticipated capabilities might not come to fruition, and other unanticipated capabilities may emerge.

Near-Term Recommendations

Recommendations for the near term are as follows:

- **Revise the BWC to include strong protections, such as independent monitoring of BSL-rated laboratories in a manner akin to chemical and nuclear weapon treaties.** How to implement this recommendation is discussed in some detail in Gerstein (2021), although Gerstein (2022) notes that this effort is unlikely to succeed because biotechnology has too important a dual-use (i.e., civilian and military) purpose that no countries have shown any appetite to institute stronger international treaties.
- **Given that improving the BWC is likely intractable politically, the United States should also pursue bilateral bioweapon treaties or otherwise divest from supporting biolabs in states likely to use bioweapons in the future.** In short, the United States should divest from labs like the Wuhan Institute of Virology if the United States and China will not enter a bilateral bioweapon control treaty (which is unlikely). Figure 2.2 in this report highlights other countries that are on the advantaged side of bioweapon strategic use, and the United States should pursue bilateral treaties with these countries or else divest from their biotechnology sectors.
- **Continue scrutinizing adversary biotechnology advancements to identify and publicize BWC violations.** The United States should continue to emphasize and monitor compliance with the BWC with an eye toward transparency and accountability for all signatories' actions.
- **Members of Congress should resist anti-vaccine populism that is at the expense of military readiness.** Congress used the fiscal year 2023 National Defense Authorization Act to order that DoD rescind its COVID-19 vaccine mandate for all service members. The proposed language in the fiscal year 2024 National Defense Authorization Act seeks to enshrine the service members' ability to refuse vaccines for religious or moral purposes. DoD and the services must ensure that troops have access to accurate information and a transparent discussion regarding the benefits and risks of vaccines, but services should retain their traditional ability to mandate medical interventions in a manner unlike that in the civilian population.
- **The U.S. government should continue to be vigilant about entities that misuse biotechnologies and should continue working to enhance the information security of IoB devices.** The United States could, for example, continue coordinating through the Department of Commerce and other agencies to put foreign organizations on its Entity List. Information security of IoB devices is of utmost priority, particularly when used by warfighters. This will be even more true if BCI fulfills its promise for warfighter enhancement, potentially with write as well as read capabilities, which will necessitate novel types of information security. Such security potentially will involve systems for full override, decoupling, or override *and* decoupling of IoB systems, as well as the creation of associated redundancies to conduct warfighting without IoB technologies if needed. The United States

should work with standards-setting organizations and engage the National Institute of Standards and Technology on this task; see, for example, National Institute of Standards and Technology, 2022.

- **Focus the allocation of funding on projects to identify and manage risks and opportunities arising from genomic surveillance.** Genomic surveillance is the most near-term opportunity for genomics technology innovation, and such surveillance of familial and population ancestry is already used for both good and nefarious purposes. Furthermore, surveillance that links genotype to phenotype (traits) is the as-yet unfulfilled promise of the HGP and is a technical task that must be completed before enhancements can be applied to a broad swath of traits.
- **DoD should develop clear guidance on integrating biological warfighting capabilities** that is analogous to guidance developed for cyber and information warfare capabilities. This should be done not only across the military services but also in collaboration with trusted allies. Providing battlefield commanders and strategic planners with a clear picture of the biological warfighting capabilities being developed and how warfighters can benefit from or be hurt by them will help planners both use those capabilities in future conflicts and prepare to defend against them.

Long-Term Recommendations

Recommendations for the long term are as follows:

- **Develop warfighting conventions on the use of IoB devices, particularly BCIs.** The BWC concerns only bacteriological and toxin weapons, but we expect that warfighting will increasingly use IoB devices. Because many of these devices are likely to become more and more intimately integrated with the human body, the need to develop rules of engagement for these devices will become critical.
- **Develop ways to employ genomic surveillance for improvements in military personnel selection or assignments.** If genomic surveillance is realized and able to provide robust measures of otherwise poorly measured aspects of human potential, then such surveillance could, for example, be a consideration to help sort candidates into job specialties. It also could potentially reduce the risk of individuals who are onboarded into the service from washing out shortly after basic training. U.S. Army washout rates are at about 6 percent at the time of writing (Baldor, 2023), and it costs the Army approximately $50,000 for each person who fails to complete basic training (Kimmons, 2018). Therefore, even a small improvement in the washout rate could result in substantial gains for cost and time efficiency for staffing the force.
- **Encourage research on mitigation strategies for novel pathogen potentialities to anticipate and counter adversary biotechnology threats.** The ultimate capabilities for bioweapons will depend on the details of how humans can and cannot be infected, and how pathogens can and cannot be manipulated. While anything is conceivable (a pathogen that makes sleep impossible, a zombie virus), bioweapons ultimately are constrained by the possible. DoD will need to take actions to stay current on the latest scientific developments in viral engineering and immunology because these developments potentially will be convertible into bioweapons.

Conclusions

Our analysis shows that several countries have advantages—when compared with the United States—in their abilities to deal with the effects of a globally released, highly air- and person-to-person–transmissible bioweapon. While democratized biotechnology may allow a malicious nonstate actor to develop a bioweapon, a country with an existing lab that handles such pathogens creates an easier path for a malicious actor. Because it is difficult to identify the origins of person-to-person transmissible bioweapons, their use by state actors is more likely. In contrast, non–person-to-person transmissible bioweapons (e.g., anthrax) are more likely to be used for terrorist and DIY goals, where attribution is paramount.

IoB technology will continue to advance, and the United States must be especially cognizant that any deployed technology can also be hacked. While this is recognized for military cyber operations, this point will be even more important when soldiers and politicians have cybernetic connections directly to their activity patterns through wearables and even connections to thought processes via BCI.

Genomic surveillance is the most likely near-term technology to affect warfighting, but genomic enhancement could have profound consequences should it become more feasible technically. The United States should continue to monitor genomic developments.

The United States has long been the dominant player in human domain biotech, but our analyses suggest that there will be more countries with emergent biotech capabilities in the near future. Because those and other countries are investing significant resources into biotechnology for the warfighter, the recommendations offered in this report should enable the United States to stay ahead in this rapidly changing landscape.

Abbreviations

AI	artificial intelligence
BCI	brain-computer interface
BSL	biosafety level
BWC	Bioweapons Convention
CDC	Centers for Disease Control and Prevention
CFR	case fatality rate
COVID-19	coronavirus disease 2019
CRISPR	clustered regularly interspaced short palindromic repeats
DIY	do-it-yourself
DNA	deoxyribonucleic acid
DoD	Department of Defense
EEG	electroencephalogram
GWAS	genome-wide association studies
HGP	Human Genome Project
HIV	human immunodeficiency virus
IoB	Internet of Bodies
mRNA	messenger ribonucleic acid
SARS-CoV	severe acute respiratory syndrome coronavirus
USSF	U.S. Space Force

References

Almeida, Mara, and Rui Diogo, "Human Enhancement: Genetic Engineering and Evolution," *Evolution, Medicine, and Public Health*, Vol. 2019, No. 1, 2019.

Baldor, Lolita C., "Basic Training Without Yelling: Army Recruits Get 2nd Chance," Associated Press, March 29, 2023.

Ball, Philip, "What the Lightning-Fast Quest for COVID Vaccines Means for Other Diseases," *Nature*, Vol. 589, December 18, 2020.

Bashford, Alison, and Philippa Levine, eds., *The Oxford Handbook of the History of Eugenics*, Oxford University Press, 2010.

Binnendijk, Anika, Timothy Marler, and Elizabeth M. Bartels, *Brain-Computer Interfaces: U.S. Military Applications and Implications, An Initial Assessment*, RAND Corporation, RR-2996-RC, 2020. As of October 2, 2023: https://www.rand.org/pubs/research_reports/RR2996.html

Biological Weapons Convention—*See* Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and Their Destruction.

Blendon, Robert J., Mary T. Gorski, and John M. Benson, "The Public and the Gene-Editing Revolution," *New England Journal of Medicine*, Vol. 374, No. 15, April 14, 2016.

Blumenthal, Marjory S., Alison K. Hottes, Christy Foran, and Mary Lee, *Technological Approaches to Human Performance Enhancement*, RAND Corporation, RR-A1482-2, 2021. As of August 2, 2023: https://www.rand.org/pubs/research_reports/RRA1482-2.html

Brown, Abram, "Security Flaw in Strava, a Social Fitness App, Exposed Identities of Israeli Soldiers at Military Bases," *Forbes*, June 21, 2022.

Browne, Ryan, "Pentagon Bans Use of Geolocators on Fitness Trackers, Smartphones," CNN, August 6, 2018.

Carlsen, William, "Did Modern Medicine Spread an Epidemic? After Decades, and Millions of Injections, Scientists Are Asking the Chilling Question," *San Francisco Chronicle*, January 15, 2001.

CDC—*See* Centers for Disease Control and Prevention.

Centers for Disease Control and Prevention, "Variants and Genomic Surveillance for SARS-CoV-2," webpage, last updated April 26, 2023. As of October 2, 2023: https://www.cdc.gov/coronavirus/2019-ncov/variants/variant-surveillance.html

Clarivate Analytics, "Web of Science," webpage, undated. As of October 4, 2023: https://www.webofknowledge.com

Committee on Human Gene Editing, *Human Genome Editing: Science, Ethics, and Governance*, National Academies of Sciences, Engineering, and Medicine, 2017.

Computational Pan-Genomics Consortium, "Computational Pan-Genomics: Status, Promises and Challenges," *Briefings in Bioinformatics*, Vol. 19, No. 1, January 2018.

Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and Their Destruction, entered into force July 15, 1976 (Biological Weapons Convention).

Dawkins, Richard, *The Blind Watchmaker: Why the Evidence of Evolution Reveals a Universe Without Design*, W. W. Norton, 1986.

de los Campos, Gustavo, and Daniel Gianola, "Genomic Prediction in the Big Data Era," *American Scientist*, Vol. 111, No. 5, September–October 2023.

Department of Commerce, Bureau of Industry and Security, "Addition of Certain Entities to the Entity List and Revision of an Entry on the Entity List," *Federal Register*, Vol. 86, No. 240, December 17, 2021.

Department of Homeland Security, "National Biodefense Analysis and Countermeasures Center," webpage, last updated January 12, 2023. As of October 2, 2023: https://www.dhs.gov/science-and-technology/national-biodefense-analysis-and-countermeasures-center

Department of State, *Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments*, April 2022.

Doherty, Thomas, "Should There Be a Human Warfighting Domain?" *Small Wars Journal*, December 3, 2015.

Dolman, Everett C., "Space Is a Warfighting Domain," *Aether: A Journal of Strategic Airpower & Spacepower*, Vol. 1, No. 1, Spring 2022.

Egloff, Florian J., *Semi-State Actors in Cybersecurity*, Oxford University Press, 2022.

Enserink, Martin, and Lei Du, "SARS. China Dumps CDC Head, Probes Lab," *Science*, Vol. 305, No. 5681, July 9, 2004.

Eusebi, Christopher A., and Richard Silberglitt, *Identification and Analysis of Technology Emergence Using Patent Classification*, RAND Corporation, RR-629-OSD, 2014. As of October 2, 2023: https://www.rand.org/pubs/research_reports/RR629.html

Fish, Tim, "Data Centric: US Army Looks to Wearable Devices for New Edge," *Army Technology*, May 5, 2023.

Gelfand, Michele J., Joshua Conrad Jackson, Xinyue Pan, Dana Nau, Dylan Pieper, Emmy Denison, Munqith Dagher, Paul A. M. Van Lange, Chi-Yue Chiu, and Mo Wang, "The Relationship Between Cultural Tightness-Looseness and COVID-19 Cases and Deaths: A Global Analysis," *Lancet Planet Health*, Vol. 5, No. 3, March 2021.

Gerstein, Daniel, "Could the Bioweapons Treaty Be Another Tool for Addressing Pandemics?" *Bulletin of the Atomic Scientists*, March 12, 2021.

Gerstein, Daniel M., "Reforming Global Pandemic Preparedness and Response Institutions," in John V. Parachini, Jennifer Bouey, Daniel M. Gerstein, Alison K. Hottes, Bradley Martin, Trupti Brahmbhatt, Katherine Grace Carman, Anita Chandra, K. Jack Riley, and Barbara Bicksler, *Lessons Learned from the COVID-19 Outbreak: Preventing and Managing Future Pandemics*, RAND Corporation, PE-A1481-2, 2022. As of October 2, 2023: https://www.rand.org/pubs/perspectives/PEA1481-2.html

Global Biolabs, "Articles," webpage, undated. As of October 2, 2023: https://www.globalbiolabs.org/articles

Goad, Mason, "A New Interactive Map Reveals Where the Deadliest Germs Are Studied," Schar School of Policy and Government, July 8, 2021.

Gürtler, Lutz G., and Josef Eberle, "Aspects on the History of Transmission and Favor of Distribution of Viruses by Iatrogenic Action: Perhaps an Example of a Paradigm of the Worldwide Spread of HIV," *Medical Microbiology and Immunology*, Vol. 206, No. 4, 2017.

Hadley, Greg, "Everything You Need to Know About the Space Force's Fitness Tracker PT Study," *Air and Space Forces Magazine*, May 25, 2023.

Hall, Stephen S., "Revolution Postponed: Why the Human Genome Project Has Been Disappointing," *Scientific American*, Vol. 303, No. 4, October 1, 2020.

Hern, Alex, "Shadowy Strava Users Spy on Israeli Military with Fake Routes in Bases," *The Guardian*, June 21, 2022.

Hinkel, Lauren, "Busy GPUs: Sampling and Pipelining Method Speeds Up Deep Learning on Large Graphs," MIT News, November 29, 2022.

Hsu, Jeremy, "The Strava Heat Map and the End of Secrets," *Wired*, January 28, 2018.

IFI Claims Patient Services, "CLAIMS Direct Data Collection," webpage, undated. As of October 2, 2023: https://www.ificlaims.com/product/product-data-collection.htm

Jin, Xiuxiu, Xinyi Guo, Jingyang Liu, Qingge Guo, Bo Lei, and Jianfeng Wang, "Smart Contact Lens with Transparent MXene Decoration for Ocular Photothermal Therapy and Eye Protection," *Cell Reports Physical Science*, Vol. 4, No. 2, February 15, 2023.

Joyner, Michael J., and Nigel Paneth, "Promises, Promises, and Precision Medicine," *Journal of Clinical Investigation,* Vol. 129, No. 3, 2019.

Kania, Elsa B., "Minds at War: China's Pursuit of Military Advantage Through Cognitive Science and Biotechnology," *PRISM,* Vol. 8, No. 3, 2019.

Kania, Elsa B., and Wilson Vorndick, "Weaponizing Biotech: How China's Military Is Preparing for a 'New Domain of Warfare,'" *Defense One*, August 14, 2019.

Kimmons, Sean, "OPAT Reducing Trainee Attrition, Avoiding Millions in Wasted Training Dollars, Officials Say," Army News Service, July 2, 2018.

Klotz, Lynn C., and Edward J. Sylvester, "The Consequences of a Lab Escape of a Potential Pandemic Pathogen," *Frontiers in Public Health*, Vol. 2, 2014.

Knight, Mariya, Olga Voitovych, Andrew Carey, Tim Lister, and Josh Pennington, "Russian Commander Killed While Jogging May Have Been Tracked on Strava App," CNN, July 12, 2023.

Koblentz, Gregory D., Mayra Ameneiros, Becca Earnhardt, Ryan Houser, Joseph Rodgers, and Hailey Wingo, *Global BioLabs Report 2023*, Kings College London and Schar School of Policy and Government, George Mason University, 2023.

Kolodziejczyk, Bart, "Do-It-Yourself Biology Shows Safety Risks of an Open Innovation Movement," Brookings Institution, October 9, 2017.

Lee, Mary, Benjamin Boudreaux, Ritika Chaturvedi, Sasha Romanosky, and Bryce Downing, *The Internet of Bodies: Opportunities, Risks, and Governance*, RAND Corporation, RR-3226-RC, 2020. As of October 2, 2023:
https://www.rand.org/pubs/research_reports/RR3226.html

Libicki, Martin C., "Correlations Between Cyberspace Attacks and Kinetic Attacks," *Proceedings of the 2020 12th International Conference on Cyber Conflict (CyCon)*, July 2, 2020.

Lin, Patrick, Max Mehlman, Keith Abney, and Jai Galliott, "Super Soldiers (Part 1): What Is Military Human Enhancement?" *Human Performance Technology: Concepts, Methodologies, Tools, and Applications*, 2014.

Mathieu, Edouard, Hannah Ritchie, Lucas Rodés-Guirao, Cameron Appel, Charlie Giattino, Joe Hasell, Bobbie Macdonald, Saloni Dattani, Diana Beltekian, Esteban Ortiz-Ospina and Max Roser, "Coronavirus Pandemic (COVID-19)," webpage, undated. As of July 26, 2023:
https://ourworldindata.org/coronavirus

Matthews, Luke J., "Thinking Outside the Altruistic Box: Why We Need Other Evolutionary Theories to Explain Why Religion Is Religious," *Journal of Cognitive Historiography*, Vol. 6, Nos. 1–2, 2020.

Matthews, Luke J., Sarah A. Nowak, Courtney C. Gidengil, Christine Chen, Joseph M. Stubbersfield, Jamshid J. Tehrani, and Andrew M. Parker, "Belief Correlations with Parental Vaccine Hesitancy: Results from a National Survey," *American Anthropologist*, Vol. 124, No. 2, June 2022.

Matwyshyn, Andrea M., "The Internet of Bodies," *William & Mary Law Review*, Vol. 61, No. 1, 2019.

Mauroni, Al, "On Biological War," *Military Review*, Vol. 102, No. 3, May–June 2022.

McGuffin, Chris, and Paul Mitchell, "On Domains: Cyber and the Practice of Warfare," *International Journal*, Vol. 69, No. 3, September 2014.

Merler, Stefano, Marco Ajelli, Laura Fumanelli, and Alessandro Vespignani, "Containing the Accidental Laboratory Escape of Potential Pandemic Influenza Viruses," *BMC Medicine*, Vol. 11, 2013.

National Academies of Sciences, Engineering, and Medicine, *Human Genome Editing: Science, Ethics, and Governance*, National Academies Press, 2017.

National Human Genome Research Institute, "Genetics vs. Genomics Fact Sheet," webpage, last updated September 7, 2018. As of October 2, 2023:
https://www.genome.gov/about-genomics/fact-sheets/Genetics-vs-Genomics

National Human Genome Research Institute, "Transcriptome Fact Sheet," last updated August 17, 2020.

National Human Genome Research Institute, "The Cost of Sequencing a Human Genome," fact sheet, last updated November 1, 2021.

National Human Genome Research Institute, "DNA Sequencing," webpage, last updated October 2, 2023a. As of October 2, 2023:
https://www.genome.gov/genetics-glossary/DNA-Sequencing

National Human Genome Research Institute, "Epigenetics," webpage, last updated October 2, 2023b. As of October 2, 2023:
https://genome.gov/genetics-glossary/Epigenetics

National Institute of Standards and Technology, "NIST Issues Guidance on Software, IoT Security and Labeling," press release, February 4, 2022.

National Institutes of Health, "The Future of Health Begins with You," webpage, undated. As of August 18, 2023:
https://allofus.nih.gov

Needham, Kirsty, and Clare Baldwin, "Special Report: China's Gene Giant Harvests Data from Millions of Women," Reuters, July 7, 2021.

Ouellette, Jennifer, "BCI Lets Completely 'Locked-In' Man Communicate with His Son, Ask for a Beer," *ArsTechnica*, April 15, 2022.

Parachini, John V., and Rohan Kumar Gunaratna, *Implications of the Pandemic for Terrorist Interest in Biological Weapons: Islamic State and al-Qaeda Pandemic Case Studies*, RAND Corporation, RR-A612-1, 2022. As of October 2, 2023:
https://www.rand.org/pubs/research_reports/RRA612-1.html

Patent and Trademark Office, "Classification Resources: Cooperative Patent Classification," webpage, undated. As of October 4, 2023:
https://www.uspto.gov/web/patents/classification/cpc/html/cpc.html

Peters, Alexandra, "The Global Proliferation of High-Containment Biological Laboratories: Understanding the Phenomenon and Its Implications," *Revue Scientifique et Technique*, Vol. 37, No. 3, December 2018.

Roll-Hansen, Nils, "Eugenics and the Science of Genetics," in Alison Bashford and Philippa Levine, eds., *Oxford Handbook of the History of Eugenics*, Oxford University Press, 2010.

Ruck, Damian J., Joshua Borycz, and R. Alexander Bentley, "Cultural Values Predict National COVID-19 Death Rates," *Springer Nature Social Sciences*, Vol. 1, No. 3, 2021.

Ruck, Damian J., Luke J. Matthews, Thanos Kyritsis, Quentin D. Atkinson, and R. Alexander Bentley, "The Cultural Foundations of Modern Democracies," *Nature Human Behavior*, Vol. 4, No. 3, March 2020.

Schmid, Eric, "The Space Force Is Scrapping the Annual Fitness Test in Favor of Wearable Trackers," NPR, August 2, 2022.

Secretary of the Air Force Public Affairs, "U.S. Space Force Unveils Name of Space Professionals," press release, United States Space Force, December 18, 2020.

Shih, Jerry J., Dean J. Krusienski, and Jonathan R. Wolpaw, "Brain-Computer Interfaces in Medicine," *Mayo Clinic Proceedings*, Vol. 87, No. 3, March 2012.

Singh, Rama S., and Bhagwati P. Gupta, "Genes and Genomes and Unnecessary Complexity in Precision Medicine," *npj Genomic Medicine*, Vol. 5, 2020.

Tucker, Patrick, "Soldiers Can Now Steer Robot Dogs with Brain Signals," *Defense One*, March 22, 2023.

van Beneden, Chris A., Harald Pietz, Robert D. Kirkcaldy, Lisa M. Koonin, Timothy M. Uyeki, Alexandra M. Oster, Deborah A. Levy, Maleeka Glover, Matthew J. Arduino, Toby L. Merlin, David T. Kuhar, Christine Kosmos, and Beth P. Bell, "Early Identification and Prevention of the Spread of Ebola—United States," *Morbidity and Mortality Weekly Report*, Vol. 65, No. 3, July 8, 2016.

Vergun, David, "DOD Investing in Wearable Technology That Could Rapidly Predict Disease," DOD News, April 28, 2023.

Walgate, Robert, "SARS Escaped Beijing Lab Twice," *Genome Biology*, Vol. 4, No. 1, 2004.

"War: The Causes of War," *Encyclopedia Britannica*, undated.

Wee, Sui-Lee, and Paul Mozer, "China Uses DNA to Map Faces, with Help from the West," *New York Times*, October 22, 2021.

Wheelis, Mark, "Biological Warfare at the 1346 Siege of Caffa," *Emerging Infectious Diseases*, Vol. 8, No. 9, September 2002.

Zegart, Amy B., *Spies, Lies, and Algorithms*, Princeton University Press, 2022.