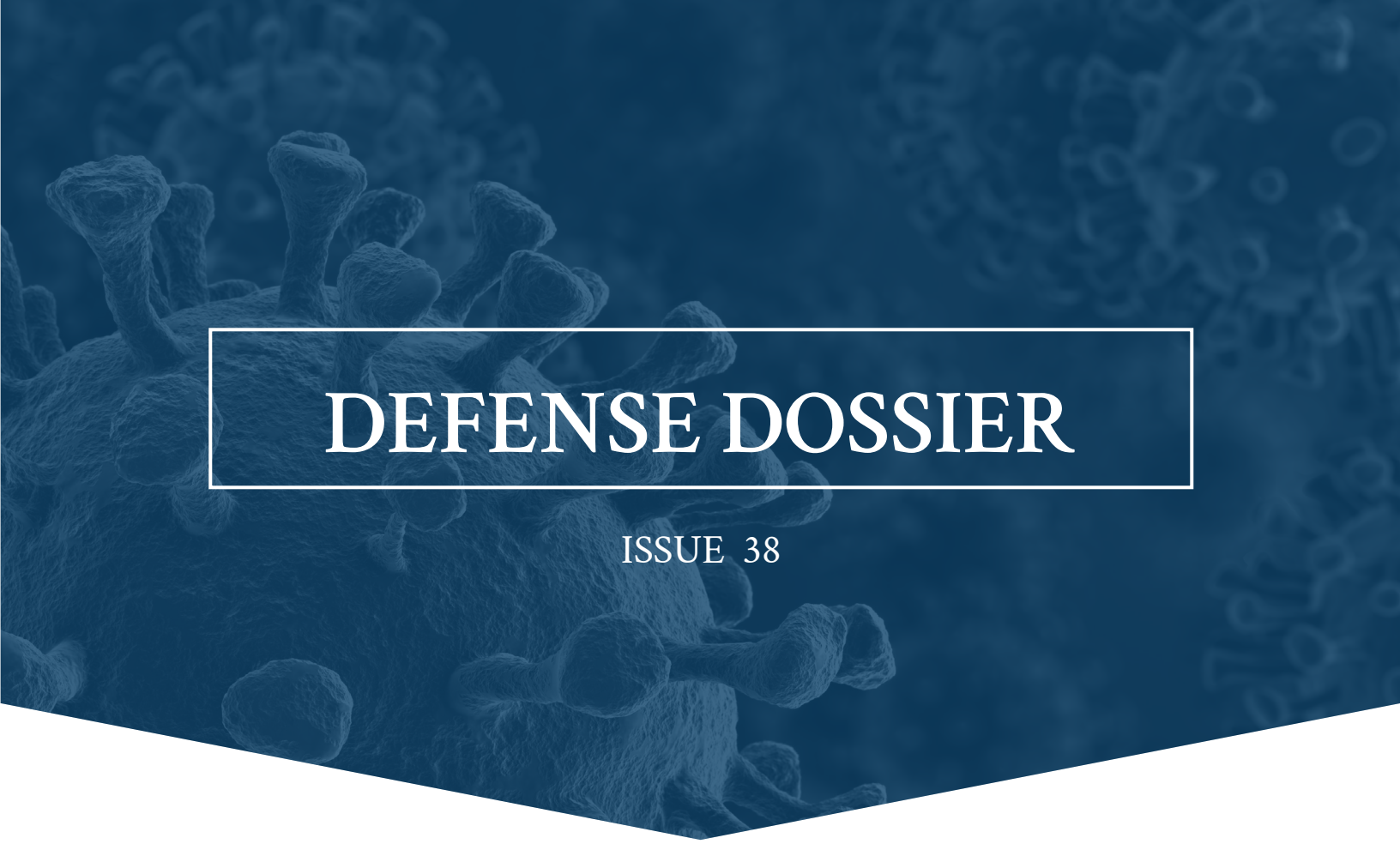

DEFENSE DOSSIER

ISSUE 38

DECEMBER 2023

AFPC

AMERICAN FOREIGN POLICY COUNCIL

AMERICAN FOREIGN POLICY COUNCIL

Explaining the World. Empowering Policymakers.

DEFENSE DOSSIER

DECEMBER 2023 | ISSUE 38

LETTER FROM THE EDITORS

Welcome to the December 2023 issue of AFPC's Defense Dossier. In this edition, we reflect on the global pandemic and its downstream effects in "Pandemic Preparedness and Biodefense."

A few years have now passed since the world suffered through the COVID-19 pandemic, allowing time to reflect on the numerous "wins" and outright failures engendered by the coronavirus. This issue opens with a discussion of the lessons learned from COVID-19. Next, we review the pros and cons of banning gain of function research, and whether eliminating it is worth sacrificing the benefits of scientific innovation. While contemplating the value of biotech, it's important to understand how our adversaries, especially China, view the issue—particularly through the lens of national security. The field's growing sophistication, meanwhile, is increasing the urgency for a better global framework to better regulate and control it. We close with an article detailing the emerging challenge posed by"cyberbiosecurity," and the novel ways in which the biotechnology and security fields intersect.

As always, we hope you find the articles engaging, enlightening, and instructive.

Sincerely,

Ilan Berman
Chief Editor

Richard M. Harrison
Managing Editor

COVID-19 Lessons Learned

Diane DiEuliis

In late December of 2019, hospitals in Wuhan, China reported fast growing numbers of patients suffering from pneumonia of unknown cause. Several weeks later, a new variant of coronavirus was identified as "severe acute respiratory syndrome coronavirus 2" (SARS-CoV-2). Although most coronaviruses are responsible for the common cold, those never before encountered by the human immune system have the potential to cause much more troubling disease symptoms. Indeed, by the end of March 2020, a pandemic of international concern was declared, spreading rapidly to almost all countries, and affecting the health of millions—putting global preparedness and response frameworks to a real-time, ultimate test.

Here in the United States, while there were numerous "wins," there were aspects of pandemic response that fell short, along with a number of outright failures. These lessons learned must chart the path forward for any future pandemic.

IT'S NOT 1918. PREPARE ACCORDINGLY

Preparedness and response experts have long used the devastatingly high death toll of the 1918 pandemic as a cautionary benchmark, along with the more recent 9/11 Anthrax attacks as obvious exemplars for why the U.S. must invest in national, state, and local preparedness for bioincidents. Indeed, the most recent version of the *National Biodefense Strategy*[1] includes naturally occurring and accidental outbreaks along with traditional bioweapons threats. The required pillars for mitigation are the same regardless of origin: early detection, prevention, preparedness, response, and recovery. While these pillars chart a modern approach to the mitigation of biological incidents, it was readily apparent during COVID-19 that the technical aspects of both preparedness and response must be "modernized" to adjust for the complexities of today's world.[2]

For instance, the delay in the development of reliable diagnostic tests by the Centers for Disease Control (CDC) wasted valuable "early warning" time. Not knowing who was infected, or where and when they were infected, necessarily meant that decisions to mitigate spread would be uneducated or reliant only on the appearance of physical symptoms. In turn, waiting for small-scale development of an approved, reliable diagnostic that could be readily deployed throughout the U.S. proved to be a detrimental bottleneck. Coupled with this, it was clear that traditional epidemiological models were inadequate in predicting complexities of disease spread. Unlike 1918, epidemiological models must now account for a much more populous society spread across both dense urban and sparse countryside geographies and traveling via multiple modes of transportation. Models must also account for daily human interaction and behavior, human biological risk factors (including genetic vulnerabilities), genetic mutations of the virus and viral adaptation over time, and seasonal and environmental variability in infectivity.

Intrinsic in the understanding of human/host biology is the ability to identify those most at-risk for the disease. Despite early indications suggesting that the most at-risk individuals were not children or healthy adults, but rather the elderly, immune compromised, or those with obesity or other risk factors, the U.S. opted to shut down its social and economic systems. This blanket approach erred on the side of not only assuming equal risk to all from COVID-19, but that the risk of infection outweighed the consequences of shutting down such systems. These assumptions turned out to be wholly incorrect.

Social cohesion and economic stability are intrinsically linked to national security and stability. In the aftermath of COVID-19, meta-analyses have shown that the effects of "lockdown" on COVID-19 mortality were large-

Dr. Diane DiEuliis *is a Distinguished Research Fellow at the National Defense University in Washington, DC.*

ly negligible, but the negative downstream outcomes were weighty.[3] Harmful health effects include increased levels of anxiety, stress and depression, and children suffering from delayed educational development. As well, lockdowns contributed to political unrest, contributed to increased incidence of domestic violence, and undermined liberal democracy. An economic impact assessment of COVID-19 by the International Monetary Fund (IMF) found that global GDP declined by more than $400 billion – leading to widespread unemployment and the collapse of many small businesses, as well as pushing more individuals into lower economic brackets (which also leads to poor public health outcomes).

How could this be avoided in future? The U.S. should invest in capabilities-based preparedness platforms, which leverage emerging biotechnologies to identify not only the early emergence of pathogens, but their infectious spread and characteristics over time. This would provide the critical data needed to implement tailored mitigation approaches (including when, how, and whether to apply social distancing), and enable the continued function of the economy and social norms. Such tools may include genomic sequencing from water, air filters, and other types of environments, in addition to testing those who are sick; further evaluations of the pathogens detected should include rapid whole genome sequencing and analysis. This data can then be paired with multivariate epidemiological analysis through bioinformatics and machine learning. Successes have already been demonstrated for wastewater testing,[4] and a comprehensive approach integrating these modernizations into a platform in Boston has also shown success.[5] The goal should be to elevate these capabilities-based tools to national level preparedness platforms, which could be bolstered in future through the use of Artificial Intelligence.[6]

It should be noted that the inability to rapidly ascertain the origin of SARSCoV2 (whether it was zoonotic or accidentally emerged from a laboratory) has done significant damage to the public's trust in its health institutions. The above outlined approach also affords forensic examination of a pathogen's characteristics, including a screen for indicators of genetic engineering or modification - the presence of which could signify laboratory origins or weaponization. This is especially relevant, given that U.S. adversaries have now readily observed U.S. vulnerabilities and negative outcomes in response to COVID-19, and may wish to replicate these outcomes through use of a bioweapon. Forensics and attribution are thus critical deterrence tools for the future of U.S. biodefense.

The required pillars for mitigation are the same regardless of origin: early detection, prevention, preparedness, response, and recovery. While these pillars chart a modern approach to the mitigation of biological incidents, it was readily apparent during COVID-19 that the technical aspects of both preparedness and response must be "modernized" to adjust for the complexities of today's world.

ENSURING ROBUST RESPONSE

Early "wins" during the pandemic were the rapid design of novel vaccine therapeutics from in *silico* genetic sequence models,[7] and the use of monoclonal antibodies and other antivirals against the original SARSCoV2 variant. However, manufacturing these treatments proved to have technical challenges. While monoclonal antibody platforms already existed, the platforms needed to produce mRNA vaccines had to be created in mid-response, and production of both medical and non-medical countermeasures writ large was limited by antiquated manufacturing methods. Despite the long-desired ability to have continuous manufacturing, COVID-19 demonstrated that it really doesn't yet functionally exist.

These vulnerabilities are inextricably linked to the

fragility of U.S. supply chains. Many of the raw manufacturing materials required were not available domestically and sourced from foreign and sometimes single suppliers overseas (the rest of the world was also reliant on these same suppliers, causing resource competition globally). This included active pharmaceutical ingredients required for vaccines, diagnostics, and other medicines, as well as resins used in the manufacture of syringes, needles, microfluidics, catheters, pipettes, moldings for manufacturing, intubation tubes, and many other supplies across all of healthcare.

Again, biotechnological modernization can remedy many shortfalls in manufacturing, which would then serve to strengthen the resilience of the supply chain. Which raw materials can be produced through biological manufacturing rather than chemical synthesis, and what platforms can, and should we build now to anticipate needs for the next pandemic? (Resins would be valuable to pursue, as making these materials through biomanufacturing also offers diversity and flexibility in how the materials can be used or reused.) A first step would be to determine the high priority raw materials which are currently outsourced to China or other suppliers and begin to synthesize them domestically.

Related to this, while it was broadly recognized that there were vulnerabilities in supply chains, there is a coincident lack of full visibility into supply chains. For example, not only is it not always known where particular raw materials come from that are utilized in the production of large-scale supplies, there are some specific US supply chains for which there is little to no visibility (for example, those for nucleic acids used in novel therapeutics such as mRNA vaccines). Coordination across supply chains is also lacking, and companies may compete for resources or customers during a global pandemic.

Capabilities-based modernization of manufacturing platforms (to include biomanufacturing), increased visibility and prioritization of supply chains, and re-shoring production will ensure more robust pandemic response in the future.

Capabilities-based modernization of manufacturing platforms (to include biomanufacturing), increased visibility and prioritization of supply chains, and re-shoring production will ensure more robust pandemic response in the future.

DEFENSE-SPECIFIC CHALLENGES

Fortunately, unlike the influenza pandemic of 1918, COVID-19 posed less of a threat to the younger, more physically fit population that serves the Department of Defense (DoD) mission. But the COVID-19 crisis nonetheless provides a lesson for future threats that may affect the military population. The DoD must modernize its own internal preparedness and response platforms, particularly so that deployed forces can have early warning and rapid availability of diagnostics[8] – the DoD may not be able to wait for external civil authority efforts to provide them.

The events surrounding the *Theodore Roosevelt* readily captured this problem. Without the ability to rapidly identify the sick, the nuclear-powered ship docked and off boarded its staff until the status of disease prevalence and spread could be determined, effectively taking the *Roosevelt* "out of the fight."[9] But the incident also revealed a more fundamental failing. The DoD has many game plans for responding to infectious threats that could have been utilized on the *Roosevelt*. Why were they not used? Routine exercising for pandemics in varied operational scenarios had lapsed and the most drastic action was taken in the face of limited understanding and testing.

But even if the plans had been executed, they may not account for the different operational roles of individuals in the military. DoD personnel work on ships, in aircraft, secure spaces, and ordinary offices, all of which may have different mitigations when those environments are infectious. As well, how should special operations forces or recruits in training facilities operate in contested environments? Many of these issues had to

be addressed on the fly during the pandemic response. To remedy this, DoD should create bioevent "campaign plans" that are biotechnology-enabled, regularly exercised, and ensure that medical and nonmedical resources, supplies and the DoD workforce are continuously sustained (thus allowing the DoD mission to be maintained). Such campaign plans could be tailored to individual mission arenas as appropriate.

The DoD may likely be the first Federal department to incorporate these lessons learned from the pandemic, given it has recently completed the first ever Biodefense Posture Review (BPR).[10] The review calls for modernized capabilities in biosurveillance and early warning, optimization of manufacturing and supply chains, visibility of medical stockpiles, and engagement of the combatant commands and services – the pivotal arenas needed to address the issues raised here. Additionally, the DoD has launched a separate biotechnology modernization program, which is focused on developing biomanufacturing capabilities for DoD's priority needs.[11] In response to federal mandates such as the Executive Order on Biotechnology and Biomanufacturing Innovation[12] and the CHIPS and Science Act,[13] the DoD will spend over one-and-a-half billion dollars over the next five years to build biomanufacturing facilities, standards, and a workforce. Whether this will benefit the DoD's biodefense needs in the near future will remain to be seen, but the investment in such infrastructure will likely go a long way to the support the modernization needed in the next pandemic.

Disclaimer: ***The views expressed in this paper are those of the author and are not an official policy or position of the National Defense University, the Department of Defense or the U.S. Government.***

ENDNOTES

[1] White House, *National Biodefense Strategy and Implementation Plan*, October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf

[2] Diane DiEuliis et al., "Beyond 1918: Bringing Pandemic Response into the Present, and Future," Institute for National Strategic Studies, National Defense University, April 27, 2020, https://inss.ndu.edu/Media/News/Article/2165914/beyond-1918-bringing-pandemic-response-into-the-present-and-future/.

[3] Jonas Herby, Lars Jonung, and Steve H. Hanke, "A Literature Review and Meta-Analysis of the Effects of Lockdowns on COVID-19 Mortality," Johns Hopkins University *Studies in Advanced Economics* 200, January 2022, https://sites.krieger.jhu.edu/iae/files/2022/01/A-Literature-Review-and-Meta-Analysis-of-the-Effects-of-Lockdowns-on-COVID-19-Mortality.pdf.

[4] Shimoni Shah et al., "Wastewater surveillance to infer COVID-19 transmission: a systematic review," Science of the *Total Environment* 804, January 15, 2022, https://www.sciencedirect.com/science/article/pii/S0048969721051354?via%3Dihub.

[5] "Homepage," Concentric by Ginkgo, n.d., https://www.concentricbyginkgo.com.

[6] Sarah R. Carter et al., "The Convergence of Artificial Intelligence and the Life Sciences," Nuclear Threat Initiative *NTI Report*, October 30, 2023, https://www.nti.org/analysis/articles/the-convergence-of-artificial-intelligence-and-the-life-sciences/.

[7] Kizzmekia S. Corbett et al., "SARS-CoV-2 mRNA vaccine design enabled by prototype pathogen preparedness," *Nature* 586, 567–571 (2020), https://doi.org/10.1038/s41586-020-2622-0.

[8] Vikram Venkatram, Diane DiEuliis, and James Giordano, "The COVID Crisis: Implications and Lessons for United States' – and Global – Biosecurity," in Ajey Lele and Kritika Roy, eds., *COVID-19: Analysing the Threat* (New Delhi: Pentagon Press, 2020), 397–405.

[9] Diane DiEuliis and Laura Junor, "Ready or Not: Regaining Military Readiness during *COVID19*," Center for the Study of Weapons of Mass Destruction *Strategic Insights*, April 13, 2020, https://wmdcenter.ndu.edu/Publications/Publication-View/Article/2147602/ready-or-not-regaining-military-readiness-during-covid19/.

[10] Department of Defense, 2023 *Biodefense Posture Review*, August 2023, https://media.defense.gov/2023/Aug/17/2003282337/-1/-1/1/2023_BIODEFENSE_POSTURE_REVIEW.PDF

[11] Undersecretary of Defense for Research and Engineer-

ing, *Memorandum: Department of Defense Biomanufacturing Strategy*, March 2022, https://media.defense.gov/2023/Mar/22/2003184301/-1/-1/1/BIOMANUFACTURING-STRATEGY.PDF

[12] White House, *Executive Order on Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy*, September 12, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/12/executive-order-on-advancing-biotechnology-and-biomanufacturing-innovation-for-a-sustainable-safe-and-secure-american-bioeconomy/.

[13] *CHIPS Act of 2022*, Public Law No. 117-167, 117th Congress, August 9, 2022, https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf

Parsing the Great Gain of Function Debate

Yong-Bee Lim and Saskia Popescu

The U.S. House of Representatives recently approved a ban on federal funding for "gain-of-function" (GOF) research. The measure limits GOF research by preventing the U.S. Department of Health and Human Services (HHS) from funding GOF research on viruses and other agents deemed to enhance pathogens of pandemic potential, and expands existing laws that limit HHS-funded GOF research in adversary countries.[1]

Some see this as a victory for safety and security, and a solid measure to ensure that, as Rep. Thomas Massie (R-KY-4) has put it, such research does not "create a cookbook, a blueprint for the next pandemic."[2] Others, however, see such a measure as disrupting scientific innovation, biomedical breakthroughs, biopreparedness efforts, and key growth initiatives on the part of the United States. They also worry that it could imperil America's drive to lead in, and be a major contributor to, the potentially $7.7 trillion emerging bioeconomy, as well as its status as a key leader in the international artificial intelligence (AI) race.[3]

THE GOF STATE OF PLAY

Numerous experts and policymakers have contributed significantly to the ongoing debate over GOF research. Many of the resulting discussions reflect points similar to those that have been made in the past. Therefore, we consider the current state of rhetoric to be one of stalemate, where proponents of GOF research and skeptics of the same are simply talking past each other, and unable to arrive at an agreeable outcome.

GOF research covers a range of activities that researchers conduct to better understand, explain, and predict how and why organisms function the way they do. Researchers conduct GOF experiments to test assumptions, confirm findings, and discover new insights by adding traits or qualities to an organism of interest. Researchers and other stakeholders then apply these findings to critical efforts – ranging from developing plants that are more salt- and drought-resistant for greater food security, to creating microbes with the unique ability to consume and degrade plastic waste, to accelerating medical treatments and prophylactics for conditions ranging from cancer and cystic fibrosis to COVID-19. In addition, GOF research furthers pandemic preparedness and outbreak response by contributing to the development of live attenuated vaccines and enhancing disease surveillance, which then strengthens medical countermeasure stockpiling and selection.

Proponents of GOF research typically use variants of the following points in their discussions: 1) that such research allows scientists to build basic scientific knowledge; 2) that it helps forecast how disease-causing organisms (known as pathogens) may be changing in nature and introducing risks to plant, animal, and human populations; and 3) that it accelerates treatment development both during and in advance of a disease event.[4]

A slice of GOF research has drawn global attention following the emergence of the COVID-19 pandemic. This type of research is called Gain of Function Research of Concern (GOFROC). Experts note that GOFROC create additional worries beyond those typically associated with GOF research, for three main reasons. First, GOFROC involves modifying pathogens to gain certain traits or abilities that may make the organism more easily able to infect and affect plants, animals, and/or people. Second, GOFROC-related pathogens typically require laboratories with greater safety and security protocols to minimize risks of personnel and environmental exposure. Third, dissemination of such research findings through the internet can be virtually instantaneous, something which makes it difficult to both determine

Dr. Yong-Bee Lim *is a Visiting Scholar at Arizona State University's College of Global Futures.* ***Dr. Saskia Popescu*** *is an Assistant Professor, Department of Epidemiology & Public Health, University of Maryland School of Medicine.*

who may access the research findings as well as to what ends the findings may be put toward. Thus, GOF skeptics say that: while such experiments do generate knowledge, the risks are not worth the knowledge gained; that there are other ways we can curb or prevent disease events, including educational, social, and cultural practices; and that such experiments have never directly provided benefits their proponents claim.[5]

While this debate may be at a stalemate, its consequences are clear. Banning GOFROC research will result in significant negative consequences to U.S. innovation and leadership in emerging spaces such as the growing bioeconomy and AI research, development, and deployment.

STIFLING INNOVATION AND LEADERSHIP

On September 12, 2022, the Biden administration announced Executive Order (EO) 14081, which calls for the U.S. government to utilize a whole-of-government approach towards U.S. biomanufacturing and biotechnology in areas such as public health, climate change, agriculture, supply chain resilience, agriculture, and national and economic security.[6] It further emphasizes how the COVID-19 pandemic demonstrated "the vital role of biotechnology and biomanufacturing in developing and producing life-saving diagnostics, therapeutics, and vaccines that protect Americans and the world," underscoring how life sciences activities are critical to security and public health efforts and how scientists apply that knowledge.[7] The implication, therefore, is that limiting GOF research will likely result in a chilling effect on U.S. innovation and leadership in this critical area.

While this debate may be at a stalemate, its consequences are clear. Banning GOFROC research will result in significant negative consequences to U.S. innovation and leadership in emerging spaces such as the growing bioeconomy and AI research, development, and deployment.

In the coming three to five years, this chilling effect can be expected to affect three critical areas. First, scientists will likely choose to avoid conducting GOF experiments out of an abundance of caution. While this may have the desired effect of limiting gain-of-function research of concern (GOFROC) experiments, it will also curb research and innovation in areas such as biomanufacturing, environmental remediation and restoration, and technologies that could replace current resource-intensive methods compared to bio-based alternatives.

Second, it will erode our ability to anticipate, respond to, and recover from biological events. The clearest example in this regard would be in researching, testing, and developing diagnostics and vaccines for current and future diseases of concern, including additional coronaviruses, influenza viruses, and other currently unknown viral and bacterial pathogens circulating in nature.

Finally, it will leave us ill-prepared for current and new threats in the biological risk space. This includes the increasing prevalence of antimicrobial resistance (AMR) found in greater numbers of bacteria, viruses, fungi, and parasites, leaving the United States and the global community at large in a vulnerable position, since pathogens and parasites no longer respond to the treatments that are currently available.[8]

UNINTENDED CHALLENGES

EO 14081 includes a call to action that focuses on developing foundational scientific knowledge and capabilities. To this end, one of the key capabilities that the U.S. and other countries are keeping close tabs on is artificial intelligence: an emerging technology, complete with its own suites of subordinate technologies, methodologies, and applications built on computer-based systems, which researchers have applied to better understand biological systems, discover new insights, and potentially harness for new discoveries and applications. Recent AI applications in the life sciences include analyzing DNA sequences to directly connect such sequences to the specific traits of an organism, and characterizing novel proteins to find potential new drugs for medical purposes.

While AI tools hold immense promise,

they also have specific requirements in order to be effective. A key requirement for robust AI applications is to train AI models with relevant research data. Currently, researchers are training AI models with studies to identify meaningful patterns for everything from healthcare to biomedical purposes. As these models are trained and refined, it is more likely that hidden patterns could emerge, leading to both a better understanding of the life sciences and promising new applications to address domestic and global issues.[10]

Freezing U.S. GOF research, however, will stymie the ability to fully leverage such breakthroughs, since the AI tools researchers are training could end up having significant gaps if researchers do not incorporate GOFROC-related information into newer models. And without comprehensive models that incorporate current and future GOF work, AI tools are less likely to predict viral evolution trends and discover promising new biomedical interventions for current and future biological threats.[11] In turn, this could result in near and peer competitors having more advanced capabilities and outcomes for using AI in the life sciences: a dynamic that would leave the United States potentially trailing behind adversary and competitor nations during a period of intense geopolitical tension.[12]

Despite their significant differences, GOF proponents and skeptics alike agree on two general topics. First, revisiting and strengthening biosafety and biosecurity measures is necessary to better balance safety, security, and innovation in the life sciences. Second, such research does provide information that researchers can use to understand biological systems and apply toward domestic and global problems.

BALANCING SAFETY, SECURITY AND INNOVATION

Despite their significant differences, GOF proponents and skeptics alike agree on two general topics. First, revisiting and strengthening biosafety and biosecurity measures is necessary to better balance safety, security, and innovation in the life sciences. Second, such research does provide information that researchers can use to understand biological systems and apply toward domestic and global problems.

As we have contended above, stymieing GOF research will have chilling effects in two critical areas of U.S. growth and innovation: the emergent bioeconomy and realizing the promise of AI.

To conclude, we provide three major recommendations for consideration. First, a persistent gap is that GOF oversight and requirements currently only apply to U.S. government-funded work. As the bioeconomy continues to grow, there will be an increase in privately-funded life sciences projects and products. While efforts are underway to build norms and practices for industry players, it will be necessary over time to place requirements for GOF oversight and requirements on all life sciences ventures, regardless of how the project or product is funded.[13] Further, there is no guarantee that limiting GOFROC in the United States will mean all other countries will follow suit. To the contrary, adversary countries may end up attracting researchers and companies due to a lack of such policies.

Second, the life sciences can enhance existing safety and security strategies through lessons learned from other sectors. One model, which has been endorsed and promoted by current and past leaders of organizations such as the American Biological Safety Association, takes lessons from the healthcare-based "just culture" approach. Just culture balances transparency and honesty through a non-punitive reporting of safety events. This approach utilizes institutional and individual responsibility to identify and analyze errors to review and build better processes and tools. This approach acknowledges the quirks of human behavior in complex systems and thus requires "a change in focus from errors and outcomes to system design and management of the behavioral choices

of all employees."[14] While this does not translate to an entirely blame-free environment, in which negligence is accepted, it identifies how systemic issues can increase risk of failure through transparency and mutual accountability. Encouraging researchers to report near-misses to ensure they are identified can help improve operational and safety protocols, and can serve as a balanced strategy to identify safety/security risks without stifling innovation.

Finally, we recommend taking alternative approaches to address existing gaps and issues in governing GOF research. Rather than putting in new guidance without adequate testing and data, one alternative is to test and adapt new governance tools. Dr. Alexander Titus, one of the Commissioners on the National Security Commission on Biotechnology and the inaugural Assistant Director for Biotechnology at the Department of Defense, has recently proposed what he calls "violet teaming" for developing AI systems: a process that combines probing for vulnerabilities in a system while iteratively designing safety and security solutions as these systems become actualized over time.[15] We assert that a similar "violet teaming" process can be developed between GOFROC researchers and safety and security experts. Building strong, repeated interactions between the researchers and the safety and security experts have numerous benefits, including more robust relationships between safety/security and researcher communities, having a better understanding of how the opportunities and risks associated with the research change over time, and developing proactive actions and activities to mitigate risks once the research is complete.

ENDNOTES

[1] Sarah Owermohle, "House Moves to Limit So-Called Gain-Of-Function Research," *STAT*, November 15, 2023, https://www.statnews.com/2023/11/15/gain-of-function-research-limit/

[2] Jocelyn Kaiser, "House Approves Ban on Gain-Of-Function Pathogen Research," *Science*, November 15, 2023, https://www.science.org/content/article/house-approves-ban-gain-function-pathogen-research

[3] World Business Council for Sustainable Development, *Circular Bioeconomy: The Business Opportunity Contributing to a Sustainable World*, November 2020,https://www.wbcsd.org/contentwbc/download/10806/159810/1

[4] David Gillum, Rebecca Moritz, Megan J. Palmer, and Sam Weiss Evans, "Why Gain-Of-Function Research Matters," *The Conversation*, June 21, 2021, https://theconversation.com/why-gain-of-function-research-matters-162493

[5] Todd Kuiken, *Oversight of Gain of Function Research with Pathogens: Issues for Congress*, U.S. Congressional Research Service, May 26, 2022, https://crsreports.congress.gov/product/pdf/R/R47114

[6] White House, "Executive Order on Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy," September 12, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/12/executive-order-on-advancing-biotechnology-and-biomanufacturing-innovation-for-a-sustainable-safe-and-secure-american-bioeconomy/

[7] Ibid.

[8] Gigi Kwik Gronvall, "Let the Experts Shape U.S. Biotech Regulation," *Lawfare*, October 29, 2023, https://www.lawfaremedia.org/article/let-the-experts-shape-u.s.-biotech-regulations

[9] Todd Kuiken, *Artificial Intelligence in the Biological Sciences: Uses, Safety, Security, and Oversight*, U.S. Congressional Research Service, November 22, 2023, https://crsreports.congress.gov/product/pdf/R/R47849

[10] Ibid.

[11] U.K. Ministry of Defense, *Machine Learning with Limited Data: Future of AI for Defence Project Autonomy Programme*, 2020, https://assets.publishing.service.gov.uk/media/5fcdf575d3bf7f5d06b02b0d/Machine_Learning_with_Limited_Data_original_version_.pdf

[12] Robert Work, "AI and Synthetic Biology are Critical to Future U.S. Competitiveness," *War on the Rocks*, May 27, 2021, https://warontherocks.com/2021/05/ai-and-synthetic-biology-are-critical-to-future-u-s-competitiveness/

[13] Kuiken, *Oversight of Gain of Function Research with Pathogens: Issues for Congress.*

[14] Philip G. Boysen II, "Just Culture: A Foundation for Balanced Accountability and Patient Safety," *The Ochsner Journal* 13, no. 13, 2013, 400-406, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3776518/#:~:text=A%20just%20culture%20balances%20the,the%20quality%20of%20their%20choices.

[15] Alexander J. Titus and Adam H. Russell, "The Promise and Peril of Artificial Intelligence - 'Violet Teaming' Offers a Balanced Path Forward," August 28, 2023, https://arxiv.org/pdf/2308.14253.pdf

China's Evolving Thinking About Biotechnology

Larry M. Wortzel

Ever since the Black Death swept over Asia in the 13th and 14th centuries, China has had experience with biological threats and warfare. In the 20th century, Japan conducted brutal biological experiments in China during World War II, leaving a permanent scar on the country's population. The result of this experience is a major contemporary emphasis on biological defenses, and on research into biological warfare programs on the part of the Chinese People's Liberation Army (PLA).

In the 21st century, new biotechnologies, synthetic genetics, artificial intelligence, and the potential for man-machine interface, have led to China's biotechnology programs evolving further. Some scholars and strategists are now exploring the offensive uses of some forms of biotechnology, while Chinese Communist Party (and Central Military Commission) Chairman Xi Jinping, with his emphasis on the integration of military and civil industry and research (军民融合),[1] has energized these programs.

Today, Chinese military strategy tends to study biological warfare and biotechnology alongside technological advances in artificial intelligence (AI) (人工智能) and biomechanics. All are part of the same problem-set, and are treated as a potential means to degrade enemy soldier performance or provide its own soldiers with advantages during military operations.

THE WEIGHT OF HISTORY

Concerns about biowarfare in China are heavily influenced by the historical experience of the Japanese attacks on China between 1932 and 1945. China experienced World War II before the U.S. and Europe. Japan's biological warfare experiments during the conflict were notorious, and included using various biological agents in places like Changde, Hunan Province and Ningbo, Zhejiang Province, ultimately killing over 10,000 people.[2] These experiments were spearheaded by General Ishii Shiro and his notorious 731 Unit. Shiro, however, was subsequently granted immunity from an international military tribunal by the U.S. government in exchange for information on the biological warfare programs he had conducted.[3]

That decision stained America's reputation in China, and its effects are still felt today; the PRC education system continues to emphasize granting immunity to Ishii as proof the U.S. has intentions to use biological weapons. There also are accusations from China (and the Soviet Union/Russia) that the U.S. covered up Ishii's research and then, itself, conducted experiments in biological warfare during the Korean War in North Korea.[4] While there is now definitive literature debunking the original accusations and showing they were Soviet propaganda that was picked up by the Chinese Communist Party, there is still a residual body of literature in China that accuses the U.S. of these things.

Ironically, despite their brutality, the biological experiments carried out in China by Shiro and his 731 Unit proved militarily ineffective. Yet today, there are Chinese military strategists, leaders, and medical personnel seriously thinking about how to improve biotechnology, and even link biotech and synthesized genetics to modern information technology and command and control systems to assist in military operations.

HOW CHINA THINKS ABOUT BIOWARFARE

Formally, China's State Council and the Chinese Ministry of Foreign Affairs maintain that China observes and upholds the Biological Weapons Convention, and will not engage in the use of biological agents in war. At the same time, suspicions of America's involvement with bioweapons and biotechnologies abound. Indeed, Chinese Communist Party periodicals charge that the United States may already be working on biological agents or human

Dr. Larry Wortzel, *a retired U.S. Army colonel, is Senior Fellow in Asian Security at the American Foreign Policy Council in Washington, DC.*

capabilities enhancement.[5]

For example, the 2017 edition of the PLA doctrinal publication, The Science of Military Strategy discusses biotechnology as an "emerging new form of strategic power."[6] Concerns about the United States and biological programs it may be conducting influence PLA thinking on the topic. The authors write that "developed countries, especially the United States, have adopted a series of measures to occupy the commanding heights of military conflict in the biological field."[7]

The type of emerging biotechnology with the greatest capacity to inflict casualties are 'genetically engineered weapons designed to attack people of a specific racial or ethnic background… to ensure people of specific races fall ill.'

The Science of Military Strategy portrays the United States as likely to engage in biowarfare because the United States is the only nation that has used nuclear weapons to achieve its wartime objectives.[8] The publication argues that an enemy's drive to achieve political objectives in war has in the past and can again lead to the use of weapons of mass destruction, emphasizing a direct link between the use of nuclear weapons and demands for the unconditional surrender of Japan in World War II.

The PLA doesn't just fear biological warfare from the United States, however. While the PLA authors behind *The Science of Military Strategy* believe that the United States may have the most active and effective state-run programs in military biotechnology, they also point out that there is a greater threat in the biological field is from biological terrorism or the use of bioweapons by rogue actors.[9] One military working group from the PLA Academy of Military Medicine concluded that, because biological weapons could be decisive on the battlefield and are "unmanned, formless, and soundless weapons," an enemy may be tempted to use them to accomplish important political objectives.[10]

Lieutenant General (Retired) Zhang Shibo, the former commander of the Nanjing Military region and a former president of the PLA National Defense University, discusses the potential for advances in both biotechnology and intelligent systems in warfare to affect human capacity in his book, *The New High Ground for War* (战争新高地). Zhang suggests that these systems can reinforce each through genetic engineering or human-machine interface to enhance soldier performance.[11] Zhang's reference in the title to the military advantage of holding high ground clearly indicates the author's belief in the importance of these innovations to future war.

Zhang predicts that the combination of developments in the "biological realm" and the "intelligentization" of operations has the potential to transform future war.[12] He writes that the type of emerging biotechnology with the greatest capacity to inflict casualties are "genetically engineered weapons designed to attack people of a specific racial or ethnic background… to ensure people of specific races fall ill."[13]

To support his assertion that developing such technology is possible, Zhang claims that in the United States, Monsanto, and DuPont laboratories are isolating the genes of people of Black, Aryan, Chinese and Arab descent. Zhang claims that it is possible that such genetically engineered technology could be turned into large-scale genetic weapons.[14]

Senior Colonel Du Chao, now retired from the Nanjing Army Command Academy, is an even more strident voice accusing the United States of maintaining biological capabilities with the intent to use them.[15] As a strategist who wrote while on the faculty of the Nanjing Academy, a major institution of higher education in the PLA, his impact is comparable to that of a well-published faculty member of a U.S. military war college. Even after his retirement, Du published an article in the CCP's military newspaper on future war.[16] He accuses the U.S. of maintaining biological weapons programs and argues that the use of Agent Orange by the U.S. in Vietnam amounted to a form of biological warfare. Du's books are widely available to students at PLA academies, universities, and bookstores, as well as to people interested in the military, and PLA leaders. Du's retirement appears to have not ended his influence among PLA readers.

Other military thinkers are exploring how advances in biotechnology and man-machine interface may weaken enemy forces through cognitive warfare. In a 2022 article, the PLA's Party-controlled newspaper, *PLA Daily*,

an officer from the Space Engineering Academy explored how cognitive operations (认知作战) could "influence, intervene, and manipulate cognitive elements of an enemy's soldiers, such as the target object's physiology, psychology, and values."[17] The idea behind this was to combine "hard attacks (that could be kinetic or cyber) on "key nodes such as the enemy's decision-making center, command hub, and reconnaissance and early warning system" while also using the "soft kill" effects of cognitive shaping, cognitive induction, cognitive intervention and cognitive control, involved in cognitive domain operations.[18] Cognitive warfare focuses on attacking the heart and mind, and PLA thinkers seek to use it to fight precise battles with layered strategies.

BEYOND BIOTECH

This discussion is part of a larger conversation among Chinese military leaders regarding how technological advances can be harnessed for battlefield dominance. That conversation today extends to the fields of artificial intelligence, cognitive warfare and soldier enhancement.

To wit, a recent article in the *PLA Daily*, the Communist Party's military newspaper, discusses the way in which "cognitive confrontation" will create a "new face" of future warfare.[19] The author notes that in "cognitive confrontation," military operations can be carried out to improve the "spiritual [morale and will] and psychological" actions and thinking of soldiers, or alternatively, attack the morale and will of enemy soldiers. The author foresees the capability to attack or counter-attack in cognitive space and "control or counter-control" the cognitive space of one's own forces or the enemy. The objective is to establish and control psychological superiority in warfare so as to bring about "the loss or reduction of the decision-making ability and will to resist of the enemy" while improving these cognitive factors in one's own forces.

A study from a PLA military medical university, meanwhile, has called for "building a new concept of combat forces" that applies "brain science" to the power of weapons and to humans to improve the chance to win.[20] And artificial intelligence (AI) figures heavily into the PLA's calculus for future war as well, with scholars emphasizing the need for "intelligent warfare" in which AI helps enhance military operations by improving decision-making in complex situations.[21]

These, and countless other examples, highlight that the PLA is exploring how to harness 21st century technologies, including biotechnologies, for military applications.

On the topic of biological warfare, the Chinese people, the CCP and the PLA bring a lot of baggage to the table. The country's World War II experience with Japanese biological experiments has left a deep scar. So, too, has the U.S. use of nuclear weapons against Japan in that conflict. That history is now built into education programs and CCP propaganda, and as a result it is likely generally accepted that the use of biological weapons is a strong likelihood in future warfare.

A LATENT CAPABILITY

On the topic of biological warfare, the Chinese people, the CCP and the PLA bring a lot of baggage to the table. The country's World War II experience with Japanese biological experiments has left a deep scar. So, too, has the U.S. use of nuclear weapons against Japan in that conflict. That history is now built into education programs and CCP propaganda, and as a result it is likely generally accepted that the use of biological weapons is a strong likelihood in future warfare. That understanding, in turn, will drive future PLA research into the topic, as well as an emphasis on strong defenses, together preparation for the potential use of such weapons if they are used against China.

Those concerns drive a number of programs: In the military and military associated policy and research institutes, serious thinking is taking

place about what potential enemies might be working on biological weapons. Meanwhile, the advance of new research and technologies to harness men and machines with artificial intelligence means that offensive programs will creep into PLA operations over time. And defensive programs can translate quickly into offensive weapons.

The U.S. cannot afford to ignore what is going on in China's defense community. Nor should U.S. policymakers or intelligence agencies accept denials from China that the PRC would never use biological weapons. Many of the concepts being explored by PLA strategists or medical researchers may never reach fruition, and they are not operationalized today. Yet they should not be dismissed, because in the future, should it come to conflict, the PLA is likely to use biotechnologies now under development to achieve its political objectives.

END NOTES

[1] On military-civil fusion, see Larry M. Wortzel, "The Limitations of Military-Civil Mobilization: Problems with Funding and Clashing Interests in Industry-Based PLA Reserve Units," Jamestown Foundation *China Brief* 19, iss. 18, October 8, 2019, https://jamestown.org/program/the-limitations-of-military-civil-mobilization-problems-with-funding-and-clashing-interests-in-industry-based-pla-reserve-units/

[2] See Robert Harris and Jeremy Paxman, *A Higher Form of Killing: The Secret History of Chemical and Biological Warfare* (New York: Random House: 2002); Anne L. Clunan, Peter R. Lavoy, and Susan B. Martin, eds., *Terrorism, War or Disease? Unraveling the Use of Biological Weapons* (Palo Alto, CA: Stanford University Press, 2008).

[3] Hal Gold, Unit 731 (North Clarendon, VT: Charles E. Tuttle Co., 1996).

[4] Milton Leitenberg, "False Allegations of U.S. Biological Weapons Use during the Korean War," in Clunan, Lavoy, and Martin, eds., *Terrorism, War or Disease? Unraveling the Use of Biological Weapons.*

[5] "US biolab transparency urged after smearing China over weaponizing COVID-19," Global Times, May 10, 2021, https://www.globaltimes.cn/page/202105/1223060.shtml ; Xiao Tianliang, *The Science of Military Strategy* (Beijing: PLA National Defense University Press, 2017), 165; "Chinese Disarmament Ambassador: Negotiations on the Verification Protocol of the Biological Weapons Convention Are Imperative," Xinhua News Agency, September 9, 2021, http://www.news.cn/2021-09/09/c_1127844030.htm.Wang Xiaoli, "How Far Is the Ban on Biological Weapons?" Xinhua, October 29, 2020; See also Ministry of Foreign Affairs of the PRC, "Joint Statement of the Foreign Ministers of the People's Republic of China and Russia on Strengthening the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction." N.d., https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202110/t20211007_9580297.html

[6] Xiao, *The Science of Military Strategy*, 165-172, 173-179. There is a 2020 version of the book out, but according to U.S. Air Force researchers, the section on biotechnology does not differ from the 2017 version. See Marcus Clay and Roderick Lee, *Unmasking the Devil in the Chinese Details: A Study Note on the Science of Military Strategy 2020* (Montgomery, AL: China Aerospace Studies Institute, 2022). https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2022-01-24%20SMS%202020%20in%20Perspective.pdf. For an English translation of the 2020 version of *The Science of Military Strategy*, see *In Their Own Words: Science of Military Strategy 2020* (Montgomery, AL: China Aerospace Studies Institute, January 2022). https://airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-6%202020%20Science%20of%20Military%20Strategy.pdf.

[7] Xiao, *The Science of Military Strategy 2017*, 171. The 2020 version contains the same language.

[8] Ibid., 171-172.

[9] Ibidem, 170.

[10] Wei Xiaoqing and Wang Yumin, "The Realistic Threat of Biological Terrorism and Medical Countermeasures (生物恐怖的现实威胁与医学对策)," *Bulletin of the Academy of Military Medical Science* 32, no. 3 (June 2008), 281-283, https://www.docin.com/p-812818691.html

[11] Zhang Shibo, *The New High Ground of War* (战争新高地) (Beijing: PLA National Defense University Press, 2017), 281-287.

[12] Ibid., 245-265.

[13] Ibidem, 231–232.

[14] Zhang, *The New High Ground of War*, 232.

[15] Du Chao, *China's Future Warfare* (中国未来战争) (Shenyang: White Mountain Press, 2012); *Du Chao, China's*

Future Warfare and Environmental Security: 21st Century Questions and Research (中国未来战争与环境安全*: 21* 世纪问题研究) (Shenyang: White Mountain Press, 2015).

[16] Du Chao, "The 36 Stratagems and Ancient Warfare: The Third Stratagem--Killing with a Borrowed Knife," (三十六计与古今战争—第三计：‘借刀杀人’) *PLA Daily,* January 18, 2018, 4, https://www.81.cn/gfbmap/content/2018-01/18/content_197224.htm

[17] Qiu Jianmin, Discussion of Psychological Warfare Tactics (心战策略论) (Beijing: PLA Academy of Military Sciences Press, 2023), 20-26, 103-115; See also Yang Longxi, "Aiming at the Future War and Fighting the Cognitive 'Five Battles' (瞄准未来战争打好认知“五仗")," PLA Daily, August 23, 2022, 7, http://81.cn/ll/2022-08/23/content_10179953.htm

[18] Yang, "Aiming at the Future War and Fighting the Cognitive 'Five Battles'," *PLA Daily.*

[19] Li Yize et.al., "Cognitive Confrontation: A New Domain of future conflict (认知对抗： 未来战争新领域)," *PLA Daily*, January 28, 2020, 3 http://www.81.cn/xuexi/2020-012/28/contyent_9726670.htm

[20] Luo Xu et.al., "Military Brain Science Factors of battle effectiveness Under a New Concept of Operation Strategies," Third Military Medical University, Chongqing, China (November 2015) Vol. 13, available through China Academic Journal Publishing House, http://www.cnki.net

[21] Yang Feilong and Li Shijiang , "Cognitive Warfare: Leading the Contest in the Era of Intelligence (人工智战：主导只能时代的较量)," *PLA Daily*, March 19, 2020, 7.

The Case for A Biotechnology Export Control Regime

Kyle Wilgus

Over the past couple of years, the COVID-19 pandemic has underscored the risk that pathogens pose to our everyday lives. Despite its robust healthcare system and global economic dominance, the United States found itself fundamentally challenged by the disease. America relied on immense financial investments and a whole-of-government approach to fight back. In hindsight, had the country been adequately prepared, there is little doubt that at least some of the pandemic's most adverse effects could have been significantly mitigated.[1]

In the aftermath of the pandemic, continued focus needs to remain on the risks posed by malicious and deadly pathogens, whether viral or biological. The latter, in particular, requires sustained and urgent attention. There is a significant concern that state and even non-state actors can harness biological technologies to weaponize pathogens and fundamentally endanger public health. Today, biotechnologies have evolved to the point that they can threaten the survival of large populations, if not civilizations.[2] To respond properly, the United States must seek novel ways of expanding oversight of these technologies and strengthening safeguards against their misuse.

BIOTECHNOLOGY: THE NEXT NATIONAL SECURITY CONCERN

In recent years, the world has witnessed a revolution in biomedical sciences and broader biotechnology. As a result of these rapid advances, medical professionals now have an increased ability to treat diseases that were previously deemed incurable. Individuals living with deadly cancers and genetic disorders now have the potential to live long and prosperous lives. Biotechnologies have also created a range of applications to extend human lives and improve standard of living.[3] For instance, biotechnologies allow for the growth of human organs and tissues, which can create a viable and enduring source for medical transplants. Additionally, these technologies allow for the quick synthetization and manufacturing of medicines and vaccines. In turn, biotechnologies provide immense benefits to the broader economy as well. In particular, when applied to agriculture, biotechnologies can improve the nutritional value of plants, decrease the need for insecticides and pesticides, and increase plant tolerance to environmental factors.[4]

While largely positive, however, these same advances can be used for nefarious purposes. Greater technological sophistication makes it easier for ill-intentioned actors to create deadly pathogens or develop biological weapons.[5] This threat potential, moreover, is amplified by current weaknesses in the international system and the patchwork nature of existing international controls. Specifically, the Biological Weapons Convention (BWC), the leading framework tasked with preventing the emergence and spread of biological weapons, has largely failed to regulate biological agents and prevent their weaponization. Whether we are discussing Russia's declared biological weapons program[6] or China's suspected one,[7] nation-states have not been sufficiently deterred from weaponizing biological agents.

The BWC has been unsuccessful mainly due to its lack of verification, enforcement, and punishment mechanisms.[8] The convention is explicitly intended to promote the peaceful uses of biological research and prevent the emergence of biological weapons. But the BWC has no capacity to verify the claims of its signatories, or to investigate potential weapons programs when evidence of such arises. For instance, although the U.S. contends that both China and Russia maintain active biological weapons programs,[9] it lacks an institutional pathway via the BWC to report these offenders or pursue punitive actions. As a result, the Biological Weapons Convention is seen as essentially a "paper tiger" that allows clandestine programs to thrive. This, in turn, has concrete security implications for the United States and

***Kyle Wilgus** is a researcher at the American Foreign Policy Council in Washington, D.C.*

the broader international system.

First, the current lack of oversight on the transfer and use of biotechnologies facilitates the development of offensive biological weapons. Under existing governance structures, malign actors have ample opportunity to acquire increasingly dangerous technologies and weaponize biological agents. Lax international controls and a failure of international institutions have meant that a range of actors now have ready access to technologies that can potentially endanger public health. Malicious actors can harness the properties of genetic engineering to create pathogens that are resistant to and can circumvent known medical treatments. To weaponize these agents, these malign actors can notably exploit publicly available information and research studies.

The potential for doing so abounds. For instance, researchers at the State University of New York created novel strains of the polio virus from publicly available biomedical information and chemicals.[10] In another telling case, individuals at the University of Alberta used online DNA fragments to synthesize a contagious horsepox virus.[11] By following these examples, ill-intentioned actors can harness publicly available information to advance clandestine weapons programs.[12] Furthermore, these actors can exploit the inherently weak cyber defenses of research facilities to gain access to sensitive information on pathogens and experimental research. Unless new protections are put in place, this permissive environment will invariably lead to the proliferation of biological agents.

Second, international organizations and regulatory frameworks at present fail to account for the effects of emerging technologies on biological weapons programs and global health security. Emerging technologies, when paired with biotechnologies, can degrade traditional barriers to weaponization. The convergence of emerging technologies, such as artificial intelligence or additive manufacturing, with biotechnologies can be catalytic—and potentially disastrous. This technological convergence can fill gaps in expertise and lead to rapid leaps in the development and weaponization of dangerous pathogens.

Finally, limited safeguards and oversight on biotechnologies exponentially increase the risk for the accidental release of dangerous biological agents. Even while undertaking peaceful research endeavors, biotechnology threatens public health as limited oversight within the international system raises the potential for accidental release. As we saw with COVID-19, pathogens can disrupt the very fabric of our society. If weaponized pathogens are released, either intentionally or unintentionally, these agents have the potential to fundamentally alter the United States, destabilize the international system, and disrupt our democracy.

NEEDED: AN INTERNATIONAL EXPORT CONTROL REGIME

To alleviate these mounting risks, the international community needs to develop effective mechanisms to better control biotechnology and protect from its deleterious effects. To this end, the United States should prioritize the development of an international biotechnology export control regime. Such an instrument, if properly constructed, can play a key role in regulating the development of biotechnologies, protecting public health, and restricting biological weapons development. Such a mechanism could also enhance international accountability by developing novel pathways to report and punish potential offenders. Current frameworks simply do not have the capacity to verify compliance and punish potential offenders. By bolstering mechanisms to verify export control compliance, the United States and its allies can help deter cheating, inhibit biological weapons programs, and promote global health security.

Whether we are discussing Russia's declared biological weapons program or China's suspected one, nation-states have not been sufficiently deterred from weaponizing biological agents.

Such an objective, moreover, can be achieved through the institutional reform of existing international agreements. For instance, the Australia Group, an international agreement seeking to ensure that exports of biological agents and dual-use technologies do not contribute to the emergence of biological weapons, can

The United States should prioritize the development of an international biotechnology export control regime. Such an instrument, if properly constructed, can play a key role in regulating the development of biotechnologies, protecting public health, and restricting biological weapons development.

be reformed and expanded.[13] The Australia Group offers immense potential as an international biotechnology export control regime. Specifically, its focus on supply-side proliferation can be broadened to encompass technological safeguards and export controls.

Whatever avenue is pursued, however, the formation of a more robust export control regime would have immense benefits, such as harmonizing technological regulations and improving the current patchwork approach that has left biotechnology vulnerable to misuse. Such a policy mechanism can also foster norms that can guide behavior on the future use and transfer of biotechnologies. Just as significantly, it would create artificial "choke points" that can limit the development of biological weapons.[14] An international export control regime can establish such bottlenecks by restricting access to advanced and sensitive biotechnologies, thereby preventing potential proliferators from quickly acquiring and synthesizing biological agents for offensive use.

AN OPPORTUNITY FOR AMERICAN LEADERSHIP

The revolutionary nature of biotechnology underscores the need for effective policy responses. Current controls simply do not have the capacity to adequately regulate the technology and protect public health. As a result, advancements in biotechnology are dangerously outpacing legal controls and frameworks.[15]

The biotechnology revolution is rapidly approaching a critical juncture. Allowing the technology to advance and proliferate unimpeded will only exacerbate current threats and vulnerabilities, with lasting implications for the United States. Imagine if the next pandemic originates from a weaponized biological agent designed to circumvent traditional medicine and vaccines. What if smallpox, a disease that is no longer vaccinated against in the United States, is released in a major American city? Such scenarios should pose a significant concern, one that requires the United States to take a proactive approach.

But here, leadership is needed. The United States can blaze the trail in creating comprehensive controls on biotechnology in ways that benefit its own national security and the public interest. If it doesn't, however, the world will reach a stage where such technology simply won't be able to be controlled.

ENDNOTES

[1] PRTM, "The impact of state and local budget cuts on Public Health Preparedness," June 13, 2011, https://nap.nationalacademies.org/resource/21809/Impact-of-state-and-local-budget-cuts-on-PHP.pdf.

[2] Loren Thompson, *Invisible Scourge: The Danger of Chemical or Biological Attack on America is Growing Fast*, Lexington Institute, June 2018, https://www.lexingtoninstitute.org/wp-content/uploads/2018/06/6.18.18-LT-Invisible-Scourge-1.pdf.

[3] "How Does Biotechnology Benefit Humanity?" PELI *blog*, July 8, 2021, https://blog.peli.com/areas-of-interest/it-science/how-does-biotechnology-benefit-humanity.

[4] U.S. Department of State, "Biotechnology," n.d., https://www.state.gov/agricultural-policy/biotechnology/#:~:text=Biotechnology%2C%20as%20applied%20to%20agriculture,and%20floods%2C%20and%20improves%20nutrition.

[5] Al Mauroni, "Synthetic Biology: The Promise and Peril of a New Dual-Use Technology," *War on the Rocks*, August 9, 2018, https://warontherocks.com/2018/08/synthetic-biology-the-promise-and-peril-of-a-new-dual-use-technology/.

[6] Jonathan B. Tucker, "Biological weapons in the former

Soviet Union: an interview with Dr. Kenneth Alibek," *The Nonproliferation Review*, Spring-Summer 1999, https://www.nonproliferation.org/wp-content/uploads/npr/alibek63.pdf.

[7] Cate Cadell, "Pentagon Biodefense Review Points to Chinese, Russian threats," *Washington Post*, August 17, 2023. https://www.washingtonpost.com/national-security/2023/08/17/bioweapon-defense-pentagon-threats-china/.

[8] Trevor Findlay, "Verification and the BWC: Last Gasp or Signs of Life?" *Arms Control Today*, September 2006, https://www.armscontrol.org/act/2006-09/features/verification-bwc-last-gasp-signs-life.

[9] U.S. Department of State, "Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments," April 2023, https://www.state.gov/wp-content/uploads/2023/04/13APR23-FINAL-2023-Treaty-Compliance-Report-UNCLASSIFIED-UNSOURCED.pdf.

[10] Andrew Pollack, "Traces of Terror: Scientists Create Living Polio," *New York Times*, July 12, 2002, https://www.nytimes.com/2002/07/12/us/traces-of-terror-the-science-scientists-create-a-live-polio-virus.html.

[11] Diane DiEuliis, Kavita Berger, and Gigi Gronvall, "Biosecurity Implications for the Synthesis of Horsepox, an Orthopoxvirus," *Health Security* 15, no. 6, 2017, https://wmdcenter.ndu.edu/Portals/97/Documents/Publications/Articles/Biosecurity_Implications_for_the_Synthesis_of_Horsepox.pdf?ver=2017-11-03-102542-867.

[12] Sophy Macartney, "Biological Threats have Evolved for the Worse, and We Are Not Prepared," Center for Arms Control and Non-Proliferation, September 1, 2023, https://armscontrolcenter.org/biological-threats-have-evolved-for-the-worse-and-we-are-not-prepared/.

[13] The Australia Group, "The Australia Group: Objectives of the Group," n.d., https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/objectives.html.

[14] Christine Parthemore and Andy Weber, "A Deterrence by Denial Strategy for Addressing Biological Weapons," *War on the Rocks*, September 23, 2021, https://warontherocks.com/2021/09/a-deterrence-by-denial-strategy-for-addressing-biological-weapons/.

[15] Gregory D. Koblentz and Rocco Casagrande, "Biology Is Dangerously Outpacing Policy," *New York Times*, February 20, 2023, https://www.nytimes.com/2023/02/20/opinion/biology-is-dangerously-outpacing-policy.html.

Understanding the Cyberbiosecurity Threat

Charles Fracchia

In the last decade, biotechnology has become irreversibly digital. Every single major step, from research to development to manufacturing, from packaging to distribution, has been accelerated and improved by digital technologies. Most recently, this digitization has kicked off data science and artificial intelligence revolutions that are allowing us to discover new drugs and materials, produce materials in a more sustainable way, and even counteract climate threats at an unprecedented scale. But as innovation roars along,[1] it is bringing with it rapid and significant changes to the threat landscape—changes that precious few across the public and private sectors are as yet examining and defending against.

Moreover, a new category of threats has emerged at the intersection of the digital and biological domains – what might be called cyberbiosecurity. While the seedlings of this threat were present even before the COVID-19 pandemic, cyberbiosecurity issues were highlighted during the crisis as among the most critical, immediate, pervasive, deniable, and affordable attack vectors against bioeconomies around the world. It has now become a critical battleground, and potentially existential threat to the U.S. bioeconomy[2] and that of its allies.

CYBERBIOSECURITY, OR DIGITAL BIOSECURITY

In trying to define the unique properties of the cyberbiosecurity threat, we have witnessed a recurrent semantic tiff that has detracted from the public sector's ability to act against these threats. This has been true with the term "bioeconomy," but also with the term at the heart of this article. The terms "cyberbiosecurity" and "digital biosecurity" can be used interchangeably, and are intended to point to the security implications arising from the convergence of the digital and biological fields.

Cyberbiosecurity threats are defined as having a biological effect, either degrading or altering the biological function itself. In fact, the most devastating cyberbiosecurity attacks are those that employ a cheap, accessible, deniable digital channel to erode the trust and integrity of the biological layer. For example, altering the digital records of a DNA sequencer to falsely indicate that the patient shows markers for a dangerous cancerous mutation,[3] or using artificial intelligence (AI) to discover novel biological threats or evade existing countermeasures,[4] steal genomic data for identification or targeting of specific individuals, or even create disinformation campaigns targeting specific biological products.[5]

A troubling dynamic in both the public and private sector is the reduction of this threat to a cyber hygiene issue, therefore denying that it affects the integrity of biological processes themselves. In the public sector, this cultural divide is particularly strong, and has severely impeded the ability to address vulnerabilities and commit adequate resources to urgent cyberbiosecurity threats.

CATALYZING EVENTS

While cyberbiosecurity concerns have progressively grown in the last few decades, as the digital and biological fields have increasingly intertwined, two events have marked major transitions in recent years.

In 2017, the NotPetya ransomware was unleashed on Ukrainian civil society by an unknown actor, though many have suggested that the attack bore the hallmarks of a Russian government-backed attack.[6] The ransomware infect-

Charles Fracchia *is the CEO of Black Mesa, a Boston-based company focusing on solving digital biosecurity challenges and bringing a new level of manufacturing assurance. He is also the chairman of the BIO-ISAC, a non-profit organization that addresses threats unique to the bioeconomy and enables coordination among stakeholders to facilitate a robust and secure industry. In 2021, the U.S. Defense Advanced Research Projects Agency (DARPA) named Fracchia to its Information Science and Technology (ISAT) Study Group, where he advises the agency on helping to anticipate as well as generate strategic surprise.*

ed Merck & Co, an American company that happened to use the Ukrainian tax and accounting software M.E.Doc, which was used to spread the ransomware. The full extent of the damage only became clear in the years following the attack. In 2017, Merck initially claimed $135 million in lost revenue,[7] only to raise its insurance claim to $1.4 billion in 2018, citing the widespread impact on operations, including halted production.[8] Ultimately, the attack was linked to a shortage of Human Papilloma Virus (HPV) vaccine (Guardasil) in the U.S. Strategic National Stockpile.[9] Merck & Co. is not believed to have been targeted or singled out as part of this attack, but instead was collateral damage.

When	Organization	Incident	Impact	Cost
Jun. 2017	Merck & Co.	Ransomware	Caused shortage of HPV vaccine	$1.4 billion
Jan. 2020	Tissue Regenix	Data breach	1 week downtime in manufacturing	22% stock price
Apr 2020	World Health Org.	Data breach	Internal data disclosed publicly	Unknown
Sep 2020	Sputnik News	Disinformation & Malware	Targeted Oxford-AstraZeneca vaccine	Unknown
Oct 2020	Dr Reddy's	Ransomware	Several weeks, halted global operations	Unknown
Dec 2020	EU Medicines Agency (EMA)	Data Breach	Pfizer regulatory filings stolen and misinformation	Unknown
Feb 2021	Oxford University	Equipment	Quality assurance equipment modified	Unknown
Mar 2021	Serum Inst. of India	IP Theft	Data stolen and other effects unknown	Unknown
Spring 2021	North American Biomanufacturer	Ransomware	Indication of sophisticated actor	>$3M + lost revenue
Jun 2022	Illumina	Software vulnerabilities	Highest severity software vulnerability affects most prevalent DNA sequencers	Unknown
Jul 2022	Emerald Health Therapeutics	Ransomware	Contract manufacturer affected, not directly the company. Company sold.	$19.3M raised
Jun 2023	Laronde	Data integrity	Startup merged with other company from the venture capital firm	>$440M raised
Jul 2023	Evotec	Ransomware	Months of downtime, worldwide operations affected, data integrity	>€10M IT costs + lost revenue
Oct 2023	23&Me (still active)	Data Breach	6.9 million users affected, data leaked	Unknown

Table 1. A non-exhaustive list of cyberbiosecurity issues that affected organizations in the bioeconomy and health sectors. It is difficult to determine the intent of attackers with precision, and in our experience, IP theft often precedes more disruptive and destructive attacks. Most, but not all, of the incidents listed are confirmed to be intentional attacks.

The impact from this event was a wake-up call for leaders across the public and private sectors that a cyberattack's collateral damage in Eastern Europe can lead to a shortage of vaccine in the U.S. Strategic National Stockpile. It demonstrated unequivocally that digital security has become an element of biological security and assurance.

Subsequently, over the course of 2020, the COVID-19 pandemic irreversibly changed the dynamics of the cyberbiosecurity threat. As SARS-CoV-2 started to spread, the race to develop and produce safe and efficacious vaccines became the absolute priority for nations around the world. Isolation, travel bans and quarantines all increased the pressure on remote, non-human means of stealing the coveted intellectual property for the vaccines.

By this point, the field had been digitizing processes for over two decades, and none of the solutions that had been developed took into account adversarial actors of any kind. To this day, authentication and encryption are exceedingly rare – nor required – in the tools used across the biological field. The backbone that underpins all modern medicine, agriculture, livestock activity, novel material development, and bio-based climate mitigations is vulnerable to simple cyberbiosecurity attacks.

It is imperative that leaders across the public and private sectors recognize that the environment has changed. Digital technology is critical to biological technology, and it must be defended. Failing to protect it means we abdicate our ability to produce safe and trustworthy medicines, and we jeopardize the continued economic growth of the U.S. bioeconomy.

Cyberbiosecurity threats are defined as having a biological effect, either degrading or altering the biological function itself. In fact, the most devastating cyberbiosecurity attacks are those that employ a cheap, accessible, deniable digital channel to erode the trust and integrity of the biological layer.

NOTABLE ATTACKS

The Bioeconomy Information Sharing and Analysis Center (BIO-ISAC)[10] has been tracking public incidents that have affected the bioeconomy internationally. We have seen attacks run the gamut, from rudimentary to sophisticated, from opportunistic to multi-year and strategic, from anonymous to plausible public attribution. We have seen intellectual property theft, financially motivated activity (E.g.: Ransomware), destructive attacks with no apparent financial motive, mis/mal/disinformation, and multi-domain nation-state threats. This diversity of actors and types of attacks is a trenchant warning of how offenders have far outpaced any defensive activities.

ACTIONS TO BE TAKEN

Beyond the urgent defensive imperative, we must recognize that tackling these threats also represents a unique opportunity for the U.S. to lead globally. It is an opportunity to share our belief that biological technologies are an engine for economic growth and a means for the invention of life-saving medicines and materials. The U.S. can help allies defend against common adversaries who attack their biomedical and bioeconomy infrastructure – infrastructure critical to both their domestic production and continued U.S. innovation. Capitalizing on this opportunity will require greater public sector attention and strong partnership across the public-private divide.

Demand stronger security provisions from instrument manufacturers

A significant contributing factor to the cyberbiosecurity threat has been the instrument manufacturers' lack of security provisions. These instruments are at the core of every single workflow, and their compromise means a product that cannot be trusted. While the FDA has recently updated its guidance regarding medical device cybersecurity,[11] it affects only a portion of the devices at risk. For example, software and hardware used to produce vaccines are not covered (e.g.: bioreactors, tangential filtration systems, liquid chromatographers, packer/fillers, etc.). At present device manufacturers are using this separation to deprioritize or to ignore vulner-

abilities outright, even when they are disclosed responsibly to the vendor. In an effort to cut costs, vendors have also largely outsourced the development of key software and hardware components, including to locations known to harbor adversary cyber activities and staff. There is an urgent need for requirements that will force vendors to a) respond to responsible disclosures, b) fix critical issues within a reasonable timeframe, c) perform regular "red-teaming," also known as "penetration testing," of their software and hardware infrastructure, and d) prohibit the development of critical hardware and software systems in countries or with companies with known ties to adversary governments.

To this day, authentication and encryption are exceedingly rare—nor required—in the tools used across the biological field. The backbone that underpins all modern medicine, agriculture, livestock activity, novel material development, and bio-based climate mitigations is vulnerable to simple cyberbiosecurity attacks.

The BIO-ISAC has suggested that using modifications to the federal acquisition rules (FARs/DFARs) may be a proportionate way to push the industry toward greater security without creating undue regulatory burden. However, if we do not act within a relatively short time (12 to 18 months), more drastic and sudden changes will become necessary to safeguard critical processes in the bioeconomy.

Regulatory landscape changes at FDA

The U.S. Food and Drug Administration (FDA) must build comprehensive cybersecurity expertise across its different centers. At present, the Center for Device and Radiological Health (CDRH) dominates the cybersecurity conversation in the agency, focusing exclusively on medical devices. The Centers for Biological Evaluation and Research (CBER) and Drug Evaluation and Research (CDER) need to build cybersecurity expertise of their own, and do so with urgency. The plethora of attacks discussed above demonstrate that our ability to produce safe and efficacious drugs depends on the regulator developing much stronger and more broadly distributed cyberbio expertise.

Expand HHS efforts to tackle cyberbiosecurity issues

Efforts at the Administration for Strategic Preparedness and Response (ASPR) are making some progress towards a more coordinated and centralized resource to tackle cybersecurity issues at the Department of Health and Human Services (HHS).[12] Strengthening and expanding these efforts to prioritize cyberbiosecurity is essential to the trust and integrity of processes across HHS. It is also critical that BARDA and FDA report into this centralized resource to minimize inconsistencies in enforcement and prioritizations of threats. These discrepancies have been—and continue to be—a major hindrance to the fixing of vulnerabilities that have direct impact on the safety of the American public's health data.

A whole of government assessment of cyberbiosecurity vulnerabilities

While the efforts at HHS ASPR are gathering steam, other U.S. government departments are virtually inactive on cyberbiosecurity. In particular, the Department of Defense and Department of Homeland Security need to act upon cyberbiosecurity threats that affect them.

With the signing of the National Defense Authorization Act (NDAA) for financial year 2023, the DoD set out requirements that any biomanufacturing investments be accompanied with process security and assurance capabilities, as well as cybersecurity protocols.[13] Unfortunately, the department has not yet moved to meaningfully tackle cyberbiosecurity issues, leaving critical infrastructure and investments in biomanufacturing undefended. A $200 million funding announcement by the undersecretary of research and evaluation aimed at biosecurity and cyberbiosecurity threats[14] seems to either have been diverted for other functions in biomanufacturing, or outright not deployed. There is an additional urgent need for the department to perform an in-depth assessment of the vulnerabilities present at currently operating DoD laboratories. The current threat landscape is

such that a cyberbiosecurity incident could conceivably enable a false flag or similar scenario that would shatter the trust of the American public in the laboratories' safety and transparency of their activities. While unsophisticated at the time, disinformation targeting some of these laboratories by U.S. adversaries was already uncovered during the pandemic.[15]

The Department of Homeland Security (DHS) does not currently designate the bioeconomy as a one of the critical infrastructure sectors on record. Following President Biden's signing of Executive Order 14081 in September 2022, entitled "Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy," debate has raged regarding the status of the bioeconomy as a critical infrastructure sector. Unfortunately, the reality is that parts of the "bioeconomy" are not currently protected by the existing definitions of critical infrastructure sectors such as the Health and Public Health, Food & Agriculture, Chemical, or Critical Manufacturing sectors. The DHS' Cybersecurity and Infrastructure Agency (CISA) should, in collaboration with relevant sector risk management agencies, establish a cross-cutting "bioeconomy" pillar that will coordinate the alerts, actions, and public-private partnerships to defend more cohesively. There have been around half a dozen threats in 2023 alone where this lack of coordination either slowed down response or impeded it altogether.

Inter-agency exercises and planning

The most consequential and worrisome threats in cyberbiosecurity exploit existing cultural and organizational seams. In March 2023, BIO-ISAC ran a tabletop exercise for senior government officials with the John Hopkins Applied Physics Laboratory (JHU APL), which illuminated the urgent need to simulate incidents and practice response playbooks.[16] The U.S. government should establish regular exercises that test the inter-agency preparedness, coordination and response capability with particular focus on director-level coordination and partnerships across agencies.

Beyond the urgent defensive imperative, we must recognize that tackling these threats also represents a unique opportunity for the U.S. to lead globally. It is an opportunity to share our belief that biological technologies are an engine for economic growth and a means for the invention of life-saving medicines and materials. The U.S. can help allies defend against common adversaries who attack their biomedical and bioeconomy infrastructure—infrastructure critical to both their domestic production and continued U.S. innovation. Capitalizing on this opportunity will require greater public sector attention and strong partnership across the public-private divide.

ADAPT, OR PERISH

Today, we find ourselves at a crossroads for the bioeconomy. Either we mobilize to defend it against cyberbiosecurity threats, or we condemn ourselves to repeat the same mistakes that have left other critical sectors vulnerable to foreign influence and attack.[17] Unfortunately, this threat is neither hypothetical nor far off in the future. The last few years have shown that attacks from nation states and cybercriminals alike are growing in number and sophistication, with devastating effect. The continued growth of the U.S. bioeconomy depends on our ability to evolve along with the threat landscape. This necessary evolution requires strong partnership across the public-private divide in order to prepare, share information, and protect public trust in these technologies. This challenge, however, is also an opportunity for the U.S. to work with its allies to create a more robust and prosperous bioeconomy

globally – and to show how the bioeconomy can serve to benefit our societies' health, food security and sustainability instead of being a tool of conflict.

END NOTES

[1] National Academies of Sciences, Engineering, and Medicine, *Safeguarding the Bioeconomy* (Washington, DC: The National Academies Press 2020), https://doi.org/10.17226/25525.

[2] Ibid.

[3] Corey Hudson and Charles Fracchia, "From Buffer Overflowing Genomics Tools to Securing Biomedical File Formats," *DEFCON27 Conference*, August 2019, https://www.youtube.com/watch?v=7du1TltZOJg.

[4] Fabio Urbina et al., "Dual use of artificial-intelligence-powered drug discovery", *Nature Machine Intelligence* 4, 189–191 (2022), https://doi.org/10.1038/s42256-022-00465-9.

[5] Federation of American Scientists Disinformation Research Group, "Vaccine news stories hosting malware disseminated across Spanish-language Twitter," September 2020, https://fas.org/publication/vaccine-news-stories-hosting-malware-disseminated-across-spanish-language-twitter/; Hussain Lalani et al., "Addressing Viral Medical Rumors and False or Misleading Information," *Annals of Internal Medicine*, July 2023, https://doi.org/10.7326/M23-1218

[6] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *WIRED*, Aug 2022, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[7] Jessica Davis, "Petya cyberattack cost Merck $135 million in revenue", *Healthcare Finance*, Oct 2017, https://www.healthcarefinancenews.com/news/petya-cyberattack-cost-merck-135-million-revenue

[8] Richard Vanderlord, "Insurers Say Cyberattack That Hit Merck Was Warlike Act, Not Covered," *Wall Street Journal*, Feb 2023, https://www.wsj.com/articles/insurers-say-cyberattack-that-hit-merck-was-warlike-act-not-covered-11675897657

[9] Paul Roberts, "NotPetya Infection Left Merck Short of Key HPV Vaccine," *The Security Ledger*, October 2017, https://securityledger.com/2017/10/notpetya-infection-left-merck-short-key-vaccine-gardasil/

[10] "Homepage," Bioeconomy Information Sharing and Analysis Center (BIO-ISAC), n.d., https://isac.bio

[11] Food and Drug Administration, "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," September 2023, https://www.fda.gov/media/119933/download?attachment

[12] Department of Health and Human Services, "HHS Announces Next Steps in Ongoing Work to Enhance Cybersecurity for Health Care and Public Health Sectors", December 2023, https://www.hhs.gov/about/news/2023/12/06/hhs-announces-next-steps-ongoing-work-enhance-cybersecurity-health-care-public-health-sectors.html

[13] U.S. Congress, "H.R. 7776 – James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 – Section 215 SUPPORT FOR RESEARCH AND DEVELOPMENT OF BIOINDUSTRIAL MANUFACTURING PROCESSES," December 2022, https://www.congress.gov/bill/117th-congress/house-bill/7776/text

[14] U.S. Department of Defense, "New Biotechnology Executive Order Will Advance DoD Biotechnology Initiatives for America's Economic and National Security," September 2022, https://www.defense.gov/News/Releases/Release/Article/3157504/new-biotechnology-executive-order-will-advance-dod-biotechnology-initiatives-fo/

[15] Austin Ramzy and Amy Chang Chien, "Rejecting Covid Inquiry, China Peddles Conspiracy Theories Blaming the U.S.," *The New York Times*, August 25, 2021, https://www.nytimes.com/2021/08/25/world/asia/china-coronavirus-covid-conspiracy-theory.html

[16] BIO-ISAC and John Hopkins Applied Physics Laboratory, "Going Viral: Bioeconomy Defense – 2023 Tabletop Exercise," November 2023, https://www.jhuapl.edu/sites/default/files/2023-11/Going-Viral-Bioeconomy-Defense.pdf

[17] David Sanger, Clifford Krauss and Nicole Perlroth, "Cyberattack Forces a Shutdown of a Top U.S. Pipeline," *The New York Times*, May 8, 2021, https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html; National Security Agency, "Iranian Cyber Actors Exploit Known Vulnerabilities to Extort U.S. Critical Infrastructure Organizations, Other Victims," September 2022, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3157562/iranian-cyber-actors-exploit-known-vulnerabilities-to-extort-us-critical-infras/; Edward Helmore, "Cyber-attack closes hospital emergency rooms in three US states," *The Guardian*, November 28, 2023, https://www.theguardian.com/us-news/2023/nov/28/cyber-attack-us-hospitals-texas-oklahoma-new-mexico.

AMERICAN FOREIGN POLICY COUNCIL

Explaining the World. Empowering Policymakers.

Ilan Berman	Chief Editor
Richard Harrison	Managing Editor
Rehna Sheth	Graphic Design and Layout

MANUSCRIPTS SHOULD BE SENT TO the attention of the Editor at 509 C Street, NE, Washington, DC 20002, or submitted via email to defensedossier@afpc.org. The Editors will consider all manuscripts received, but assume no responsibility regarding them and will return only materials accompanied by appropriate postage. Facsimile submissions will not be accepted.

EDITOR'S NOTE: The opinions expressed in the *Defense Dossier* (ISSN 2165-1841) are those of the author(s) alone and do not necessarily represent the opinions of the American Foreign Policy Council.

ABOUT THE AMERICAN FOREIGN POLICY COUNCIL

For more than four decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

DEFENSE DOSSIER ISSUE 38