UNCLASSIFIED

A FRAMEWORK FOR BIOLOGICAL WEAPONS DETERRENCE

Center for the Study of Weapons of Mass Destruction
Institute for National Strategic Studies
National Defense University

August 2025

UNCLASSIFIED

A Framework for Biological Weapons Deterrence

"Deterrence operations convince adversaries not to take actions that threaten U.S. vital interests by.... credibly threatening to deny benefits and/or impose costs, while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome."

Department of Defense, *Deterrence Operations Joint Operating Concept*,

Version 2.0, December 2006.

Key Points

- The United States does not currently have a holistic strategy to deter biological weapons (BW) threats.
- Due to the present and growing threat of deliberate adversary use of BW against the United States (including U.S. forces, citizens, and interests) and/or against U.S. allies and partners, it is imperative that the United States deter adversaries who are or may be developing and contemplating use of BW.
- The current U.S. approach to deterring BW threats is weighted heavily toward deterrence by denial strategies rather than deterrence by cost imposition strategies.
- Deterrence of BW by denial is, on its own, a risky strategy given the significant challenge of providing adequate and reliable population defense against the full range of virulent biothreats.[1]
- While denial is an essential aspect of deterrence against BW, it should be part of a broader deterrence strategy that also includes cost imposition elements utilizing multiple tools of national power, to include military, diplomatic, and economic.
- U.S. investment in its bioeconomy, especially in emerging biotechnologies and biomanufacturing, can strengthen deterrence by denial by bolstering biodefense capabilities and associated supply chains.

This NDU INSS CSWMD research project was sponsored by the Defense Threat Reduction Agency (DTRA). NDU INSS CSWMD thanks DTRA for their sponsorship of the Center's research on deterrence, WMD, and counter-WMD issues. The views expressed in this report are those of the CSWMD authors' and do not necessarily reflect the official policy or position of DTRA, the Department of Defense, or the U.S. Government.

TABLE OF CONTENTS

INTRODUCTION

"Current biological agents and rapidly advancing biotechnology underscore the diverse and dynamic nature of deliberate biological threats. Rapid advances in dual-use technology, including bioinformatics, synthetic biology, nanotechnology, and genomic editing, could enable development of novel biological threats."

Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, February 2024**.**

The United States and its allies and partners face a rapidly expanding array of biothreats, to include the potential employment of increasingly sophisticated and lethal biological weapons (BW). Given the potentially devastating costs of a major BW attack, deterring these types of attacks is simultaneously an urgent national security priority and also an increasingly challenging mission set. At present, however, the United States lacks a holistic BW deterrence strategy. The U.S. Government faces challenges in keeping pace with the growing capability requirements to deter these types of attacks; moreover, it has not fully promulgated, implemented, or communicated a whole-of-government deterrence strategy for current or emerging BW threats. **This study was undertaken to examine current deterrence tools for BW, through original research, subject matter interviews, and the completion of two roundtable workshops held at National Defense University in the winter/spring of 2025.**

This paper:

- Describes the Department of Defense's (DoD) framework for, and present approach to, deterrence, to include the key components of an effective deterrence strategy.
- Discusses the history of the U.S. Government's approach to BW deterrence.
- Describes ways and means associated with the current U.S. government approach to defending against biothreats.
- Identifies key challenges an effective U.S. BW deterrence strategy will need to address.
- Describes findings and discussions from two roundtables held with subject matter experts from across the Interagency and other stakeholders.

Implementing an effective deterrence strategy to address metastasizing biothreats will require a whole-of-government approach, to include the expertise and capabilities of the DoD's U.S. Government Interagency partners. The DoD cannot deter BW threats acting alone. The DoD's deterrence framework, however, provides a useful model for conducting a preliminary assessment of the U.S. Government's present approach to deterring biothreats. In addition to potentially identifying possible seams and gaps within this approach, it can also help catalyze discussions and engagements across the U.S. Government aimed at improving and bolstering ways and means to realize a robust BW deterrence strategy.

BACKGROUND

DOD APPROACH TO DETERRENCE

The U.S. Government focuses significant attention and resources on preventing and preparing to respond to biological incidents, whether naturally occurring, accidental, or deliberate in origin.[2] While naturally occurring pandemics represent the historical bioincidents of greatest magnitude, the U.S. Government is growing increasingly concerned about the potential for biothreats deliberately employed by bad actors with the intent to impose costs against the United States and/or U.S. allies and partners. For this reason, although the U.S. Government has extensive preparedness strategies for responding to bioincidents of all origins, deterrence of biological weapons (BW) use is becoming a more central consideration in the biodefense mission.

Deterrence aims to influence an adversary's decision calculus to prevent hostile action by convincing an adversary that:

- The expected benefits of action are not likely to be achieved or are not worth the costs (deterrence by denial);
- The costs of action will be unacceptably high (deterrence by cost imposition); and/or,
- The outcome of *not* taking action will be acceptable (deterrence by encouraging restraint).[3]

Per the Department of Defense's *Deterrence Operations – Joint Operating Concept*, these represent the three ways of deterrence.[4]

Figure 1. Defining the 4 C's of Deterrence

In turn, the development and implementation of an effective deterrence strategy requires four elements: capabilities, communication, comprehension, and (dependent on all elements working together) credibility (sometimes referred to as the four "Cs" of deterrence (Figure 1)). Realizing all four elements and tailoring them to craft effective deterrence strategies for different potential adversaries represents a significant—but critical—challenge for the DoD and the U.S. Government.

PAST U.S. APPROACH TO DETERRING BIOLOGICAL WEAPONS

Retirement and Dismantlement of U.S. BW Program

In 1969, President Richard Nixon decided to eliminate the U.S. offensive BW program. While a number of factors contributed to the decision, by the late 1960s the U.S. Government concluded BW had little military utility, biological attacks could be deterred with nuclear or chemical weapons threats, and the political benefits of giving up BW outweighed the potential risks or costs of maintaining the program.[5] At that juncture, U.S. investments against biothreats began to shift to a defensive rather than retaliatory focus.

Post-Cold War and 9/11

After the fall of the Soviet Union and the end of the Cold War, the United States' initial primary BW concern became potential proliferation of these types of weapons due to fragile or failed states. The 1991 Persian Gulf War, however, also drew attention to the fact that the United States did not have any comprehensive or integrated deterrence strategy against BW threats. U.S. military leaders believed that Saddam Hussein would only employ such weapons in extreme desperation, and likely to limited military effect. But they also recognized that such threats, if wielded against vulnerable logistics support personnel and/or the civilian populations of partner countries, could pose potentially disastrous consequences for coalition cohesion.

While the U.S. Government continued to retain its concerns about rogue states throughout the 2000s, 9/11 and the anthrax postal attacks (also known as the Amerithrax attacks) in 2001 galvanized U.S. attention on bioterrorism. In the decade following 9/11 and the Amerithrax attacks, the United States greatly intensified its investments in countering bioterrorism. Congress significantly increased funding for bioterrorism domestic preparedness efforts and developed a series of new authorities, initiatives, and funding mechanisms to improve national public health preparedness at all levels of government and society.[6] The George W. Bush Administration and Congress together established the Department of Homeland Security as the lead federal agency for national preparedness, and the former also promulgated new national guidance and strategies for homeland security and biodefense.

The Bush-43 Administration also prioritized the development and deployment of biosurveillance technology and the expansion of national medical countermeasure programs. [7] The Obama Administration largely continued this emphasis on bioterrorism as new federal and state programs took root to counter this specific threat. [8]

This sustained momentum, coupled with the unique difficulties of deterring terrorists through threats of punishment, helped to weight the U.S. approach to defending against biothreats (to include potential BW) on the side of denial capabilities, an emphasis which has lasted up to the present day. Another factor contributing to this approach was the longstanding trend (dating back to the Nixon administration) of the United States focusing on BW threats originating from, and/or potentially employed by, actors other than major state adversaries.

2023 Biodefense Posture Review

In light of emerging biological threats, as well as lessons learned from the COVID-19 pandemic, the DoD launched its inaugural Biodefense Posture Review (BPR) in early 2023. The Review's public-facing report was published in August 2023.[9] The strategic focus of the Review was to develop a collective approach to biodefense. Its primary goals were enabling the mission effectiveness of the Total Force, prevailing (if necessary) in biologically threatened environments, and supporting a broader approach to integrated deterrence and campaigning. The BPR also sought to encourage greater collaboration with allies and partners.

While recognizing the need to expand the scope of, and participation in, developing a more robust national biodefense posture, the Review's lines of effort were primarily aligned to deterrence by denial. These included risk awareness and early detection; enterprise capabilities for prevention; preparedness to reduce impacts; and, the ability to respond rapidly and to facilitate recovery.

The BPR represented a critically important first step by the DoD to survey and organize its approach to biodefense. Even in the two years since the Review's completion, however, continuing rapid advancements in biotechnology have increased the ability of state or non-state actors to develop new and lethal BW. As a result of these and other developments, this report recommends the U.S. Government: a) assess its present approach to deterring BW, and b) develop a comprehensive, whole-of-government BW deterrence strategy.

PRESENT WAYS AND MEANS FOR BIODEFENSE

The United States has a broad range of ways and means for biodefense. Many of these ways and means represent potential components of, or could otherwise contribute to, the development of a holistic deterrence strategy for current and emerging BW threats. This section provides a general description of where current ways and means for biodefense could fit into a deterrence framework.

Deterrence by Denial

Deterrence by denial ways and means fall into three broad categories:

1) Active denial: Ways and means to directly short-circuit, intercept, engage, and defeat an attack;
2) Passive denial: Ways and means to protect a target (whether individuals/populations, equipment, facilities, broader infrastructure, etc.), such that if an attack occurs and reaches its target, its effect will be limited or negligible because it is shielded, hardened, immune, or otherwise resilient;
3) Denying the benefits of covert or deniable actions: Ways and means to ensure an attack is recognized and attributed to the attacker (and other parties responsible for facilitating or directing an attack).

With regard to BW threats, the present U.S. approach to deterrence by denial includes several ways and means that fall under these categories.

1. Active Denial of Biothreats

The U.S. Government has developed ways and means intended to prevent biothreats from originating, maturing, or proliferating. A range of counterproliferation programs and activities, for example, seek to address BW and other forms of WMD. These include the Proliferation Security Initiative (PSI), the Cooperative Threat Reduction (CTR) program, and other U.S. Government efforts to interdict proliferators and build the capacity of allies and partners (to include through exercises and education and training

initiatives) to carry out actions such as preventing dual-use components or materials from being sold or transferred to rogue states or violent extremist organizations.

2. Passive Denial of Biothreats

While the United States seeks, wherever possible, to prevent biothreats from reaching military or civilian populations, it also takes steps to help strengthen the ability of these populations to respond to and recover from exposure to these threats. This category also includes ways and means to attempt to limit and mitigate the spread of biothreats after they begin to impact and afflict a population. These goals are primarily articulated in the National Biodefense Strategy and Implementation Plan,[10] and White House Security Memorandum 15.[11] These strategies include:

- Public health measures:
    - Effective communication of key health information (to include basic prevention and protection guidelines) to the public.
    - Planning, investing, exercising, and training public health personnel and first responders to manage biothreat crises, treat mass casualties, and conduct risk communications.
    - Developing, producing, and distributing diagnostic materials and medical and non-medical countermeasures, engaging in decontamination, waste management, and other methods of suppressing pathogens during a biological event.
    - Development and distribution of vaccines or other therapeutics.
    - Preventing the release of potential biothreats through better securing or protecting biological research labs, hospitals, or other relevant facilities.
    - Facilitating recovery from biological events.
- Military force protection measures:
    - Providing personnel with relevant personal protective equipment.
    - Provision of prophylactics (both for general force health protection of warfighters and civilians) as well as vaccines or other prophylactics for those most likely to be exposed to potential bioweapons.
    - Ensure forces maintain stockpiles of key therapeutics and antimicrobial agents.
    - Filtration systems or other measures to protect bases, ships, and assigned personnel.
    - Education and training programs focused on the development of subject matter expertise in biodefense and biological threats, with tiered training for warfighters, first responders, planners, and senior leaders.
    - Education and training initiatives and exercises focused on preparing to address adversaries equipped with, and/or battlefields contaminated with, chemical, biological, radiological, or nuclear (CBRN) weapons.[12]
- Building allied and partner capacity initiatives:
    - Aiding allies and partners in developing or improving capabilities to detect, diagnose, report on, and respond to bioincidents.[13] Also includes, on the part of U.S. forces, capacities to fight and prevail in contaminated environments, as well as forensics and attribution capabilities.
- Bolstering the industrial base and associated research and development activities:

    - Investing in biodefense-relevant sectors (e.g., public health, veterinary, science and technology) to support development of a range of response and recovery capabilities and operations.
- Multilateral and international initiatives:
    - Development of international biosafety and biosecurity (see NIST biosecurity definition)[14] standards.
    - Updating export control regimes.
    - Strengthening international treaty regimes, such as the Biological Weapons Convention.

3. Denying the Benefits of Covert or Deniable Actions By Potential Adversaries

The U.S. Government also has a number of ways and means focused on identifying and attributing biothreats. These include capabilities and processes to forecast, assess, identify, characterize, monitor, and communicate essential information related to biological threats. This allows the U.S. Government to anticipate potential biothreats, enable early detection, provide early warning, support timely and impactful leadership decision-making, and accurately attribute the origin or source of these types of threats.

Specific means associated with this approach include:

- Biological monitoring and detection procedures and systems;
- Processes and personnel to collect biological data;
- Processes and systems to share epidemiological and other relevant data quickly, accurately, and securely;
- Bioforensics capabilities, to include training of law enforcement personnel for the purposes of investigating perpetrators of potential biothreats;
- Outreach to and education of state and local public and private health personnel and other first responders to recognize BW indicators;
- Programs to build awareness and detection capabilities and capacity of allied and partner states;
- Dedicated intelligence analysts and capabilities to monitor potential adversary BW programs.

An important aspect of the revised National Biodefense Strategy is that it now covers naturally occurring, accidental, *and* perpetrated biothreats; to date, however, the bulk of the above initiatives have focused on the detection of naturally occurring events. Many of these approaches are not specifically designed or oriented toward detecting and attributing BW (and/or may not be equipped to detect new forms of BW developed by a well-resourced actor such as a major state adversary), although they provide the United States with some capacity to do so in the event of a potential attack.

Deterrence by Cost Imposition

Deterrence by cost imposition (or punishment) refers to a strategy of dissuading adversaries from carrying out a specific action by communicating that considerable costs will be levied against them in response to this action. To be credible, the United States and/or its allies require the capabilities and political will necessary to impose these costs on the perpetrator.

In terms of deterring potential BW attacks through deterrence by cost imposition, within United States subject matter expert communities, past considerations or discussion of this type of deterrence generally

fell into two broad categories. (Importantly, as the United States no longer maintains an offensive BW program, any U.S. response to a BW attack will not employ commensurate means.)

i. Nuclear Weapons. The 2022 *Nuclear Posture Review* states: "Consistent with prior reviews, our nuclear strategy accounts for existing and emerging non-nuclear threats with potential strategic effect for which nuclear weapons are necessary to deter. We concluded that nuclear weapons are required to deter not only nuclear attack, but also a narrow range of other high-consequence, strategic level attacks. This is a prudent approach given the current security environment and how it could further evolve."[15]

While BW are not expressly mentioned, an adversary viewing their potential employment as causing "strategic effects" might conclude the U.S. nuclear deterrent force is relevant to U.S. BW deterrence strategies.

A past case where the implication of nuclear retaliation may have deterred battlefield use of BW was President George H.W. Bush's 1991 letter to Saddam Hussein prior to Operation *Desert Storm*, which stated, "the United States will not tolerate the use of chemical or biological weapons."[16] According to then-Secretary of State James Baker (who delivered the letter), it "purposefully left the impression that the use of chemical and biological agents would invite tactical nuclear retaliation."[17]

This threat, however, was communicated to a non-nuclear weapons state; the United States possessed a clear edge, whether in terms of escalation dominance or destructive capabilities, over Iraq. The escalation dynamics and cost-benefit assessment of a potential adversary equipped with nuclear weapons and BW might differ. This type of actor could, for example, assess its own nuclear weapons would deter the United States from launching a nuclear counterstrike in response to a BW attack.

ii. Conventional weapons and counterproliferation actions: The United States possesses a wide range of conventional weapons to impose potential costs on an adversary in response to a BW attack. Although there is not direct precedent for a U.S. conventional response following a BW attack, in April 2018—following a Syrian government chemical weapons attack on its own population—U.S. and allied air forces carried out several air strikes against Syrian research and weapons storage facilities associated with the Assad regime's chemical weapons arsenal.[18]

iii. Non-kinetic responses: Either alone or in conjunction with kinetic means, non-kinetic means can impose costs on an adversary in response to a BW attack. The efficacy of these measures and their deterrence value may vary widely between actors. For instance, an actor that is reliant on trade with the United States would be far more vulnerable to these costs than a state like Russia, which is already subject to several non-kinetic cost imposition measures. Some non-kinetic options include:

- Economic measures: Sanctions, asset seizure/freezing, and trade restrictions.
- Legal challenges: United Nations Security Council action for BWC violation(s).
- Reputational: Inflicting diplomatic and political fallout/consequences.

Deterrence by Encouraging Restraint

Deterrence by encouraging restraint refers to ways and means by which the United States can persuade a potential adversary there are benefits (or that there are not penalties) for taking a course of action, to include doing nothing, that is an alternative to a harmful action. The successful negotiation of arms control treaties, for example, may reflect a potential adversary concluding that agreeing to join an accord (and committing to not develop weapons it might otherwise have fielded and employed) is a better course of action than risks or costs associated with remaining outside of a treaty regime. The success of the United States, together with other interested governments, in negotiating the BWC and convincing most of the

world's states to join the multilateral accord (which entered into force in 1975) can be viewed as an example of encouraging the majority of the international community to foreswear developing BW.

The BWC, however, is not necessarily a strong example of this type of deterrence for a number of reasons, to include the fact most BWC member states had no interest in developing national BW programs prior to signing and ratifying the treaty.

CHALLENGES FOR U.S. DETERRENCE OF BW

The risks and costs associated with a potential BW attack against the United States and its allies and partners are rising. The United States, however, faces a number of challenges to developing and implementing an effective BW deterrence strategy. Potential adversaries, to include major state actors, are pursuing BW programs. In addition, while the United States has invested in capabilities and competencies to deter by denial—and possesses potential capabilities applicable to deterrence by cost imposition—it has not clearly communicated a BW deterrence strategy to potential threat actors. These and other challenges raise a number of questions for the DoD and U.S. Government Interagency to consider in working toward the development and implementation of a BW deterrence strategy to address current and emerging BW threats.

DETERRENCE TARGETS: BIOTHREAT ACTORS

Today, China and Russia rank as the top biothreat states of concern to the United States. But little is known about these countries' specific biothreat capabilities, strategies, or employment doctrines.

Russia

The Soviet Union first pursued BW after World War II (WWII); it perceived military utility to these weapons and also sought to match the joint BW capabilities of the United States, United Kingdom, and Canada.[19] The Soviet Union continued its BW program even after joining the BWC and after the United States renounced its own BW program (a renouncement the Soviets did not regard as credible).

In 2012, as Russia's relationship with the West severely deteriorated, Vladimir Putin announced Moscow's intent to pursue a number of exotic weapons, including weapon systems based on "genetic principles".[20] Given that Moscow continues to pursue exotic weapons systems and engages in nuclear saber-rattling to shield its extraterritorial military aggression, it is possible that the Kremlin retains BW as a potential deterrent and/or as a plausibly deniable attack method for regional conflicts.

Russia, known for "false flag" narratives, also has a long history of engaging in information manipulation pertaining to supposed U.S. BW development and use.[21] Indeed, the Kremlin reacted to the U.S. 2023 BPR by stating the release of the document confirmed that "America has something to hide."[22]

In addition, Russia has an active biological sector and was the first to approve a COVID vaccine (although it did so before clinical trials were completed); Russia's naming the vaccine "Sputnik V" suggests that Moscow views itself in a biology "race" with the United States and the West, although its biotechnology sector is not on par with that of the United States.[23]

Importantly, the 2024 U.S. State Department report on *Adherence to, and Compliance with, Arms Control, Nonproliferation, and Disarmament Agreements and Commitment* stated:

> The United States assesses that Russia maintains an offensive BW program and is in violation of its obligations under Articles I and II of the BWC. Russia continues to engage in activities prohibited by

Article I of the BWC. Russia has not fulfilled its Article II obligation to destroy or to divert to peaceful purposes BW items specified under Article I of the Convention.[24]

China

Like Russia, China views itself in a biological sector competition with the United States. In contrast to Russia, China has one of the world's largest and most powerful biotechnology sectors and has made investing in its bioeconomy a national priority.[25]

China also has a history of ethically problematic biological research efforts and engages extensively in biological dual-use research of concern, leading the United States to question Beijing's compliance with the BWC. Per the unclassified 2024 *Annual Threat Assessment of the U.S. Intelligence Community*, "China probably possesses capabilities relevant to chemical and biological warfare (CBW) that pose a threat to U.S., allied, and partner forces as well as civilian populations."[26]

In addition, the Department of Defense's 2024 *China Military Power Report* states: "As part of its historical biological weapons program, the PRC had reportedly weaponized ricin, botulinum toxins, and the causative agents of anthrax, cholera, plague, and tularemia," while noting Beijing has never provided any information on past possession of, or decommissioning of, BW programs (i.e., reporting that the Chinese government is obligated to provide, if it had BW programs in the past, because of its membership in the BWC).[27]

China's views of BW and their potential military utility are likely shaped by its experience of being the recipient of BW attacks from the Japanese in WWII and, more recently, by the struggles encountered by many governments (to include its own) in attempting to respond to the COVID-19 pandemic.[28] Some Chinese military scholars consider biology a "domain" of military conflict and have shown interest in BW as asymmetric capabilities that could potentially contribute to strategic deterrence[29] and to achieving operational advantage in conflict.

DoD's 2023 BPR expresses concern specifically in China's demonstrated interest in genetic engineering, brain sciences, and other biological research with possible military applications.[30] (In addition, China, like Russia, also responded to the 2023 BPR with false information regarding U.S. biological activities.[31])

Other Actors

Other actors of proliferation and BW concern include North Korea and Iran.

North Korea: The Democratic People's Republic of Korea is judged to maintain an active BW program, the specifics of which are a "dangerous blank spot."[32]

Iran: Tehran is currently judged to maintain a latent BW capability, although its primary "fascination" is its chemical weapons program.[33]

U.S. BW DETERRENCE COMMUNICATIONS: UNCLEAR AND INCOMPLETE

Over the course of the 21st century, the U.S. government has publicly communicated its approach to defending against biothreats through national biodefense strategies and counter-WMD strategies released by the White House and DoD. These include the 2002 *National Strategy to Combat Weapons of Mass Destruction*, the 2004 "Biodefense for the 21st Century" strategy, the 2009 *National Strategy for Countering Biological Threats*, the 2014 DoD *Strategy for Countering Weapons of Mass Destruction*, the 2018 and 2022 *National Biodefense Strategy*, the 2023 DoD *Strategy for Countering Weapons of Mass Destruction*, and the 2023 BPR. Most of these statements, however, do not expressly discuss deterrence of BW threats.

A relatively recent change in deterrence communication is the tailoring of these communications to include references to specific potential adversaries. None of the biodefense strategies from the Bush, Obama, or first Trump Administrations mentioned any potential adversary by name; rather, these documents generally referenced rogue states, failed states, and hostile non-state actors. The 2022 *National Biodefense Strategy and Implementation Plan for Countering Biological Threats, Enhancing Pandemic Preparedness, and Achieving Global Health Security* likewise did not address any potential adversaries by name; however, in contrast with previous strategies, it did include deterring bioweapons as a separate, distinct objective.[34]

Beginning in 2023, however, DoD public-facing reports and strategies on biodefense issues changed their approach. Specific potential adversary states are now included by name. Within the 2023 CWMD Strategy and 2023 BPR, DoD noted a shift in its threat focus from violent extremist organizations and regional rogue states to near-peer competitors—specifically utilizing the language of the 2022 *National Defense Strategy* by referencing China as the "pacing challenge" and Russia as the "acute threat".[35]

The 2023 BPR also marked a change with the DoD stating it would take a more visible, central, and unified role in countering adversarial biothreats.[36] While the DoD always implicitly had this role as part of broader efforts to counter, defend, and defeat the full spectrum of WMD threats, the express public identification of the Department's countering biothreat role (and the growing importance of this role) was a subtle but important change from previous public-facing documents. The DoD now emphasizes that biological (and chemical) defense is a "daily" task to be carried out by the "Total Force" rather than by specialized units alone.[37] In line with this shift, DoD has made clear it is focusing efforts to "prevent potential adversaries from developing and exploiting an area of perceived asymmetric advantage across the spectrum of conflict," including by preparing "to conduct large-scale operations in a WMD-contested environment."[38]

In addition, in recent years the U.S. Government has also devoted more attention to publicly communicating its bioeconomy priorities.[39] Such efforts can contribute to a tailored deterrence strategy by highlighting U.S. prioritization of industrial and technological capacity to strengthen all aspects of biodefense. The Obama Administration released the first comprehensive vision for the bioeconomy in 2012 with the release of the National Bioeconomy Blueprint.[40] The first Trump Administration built on this early momentum by expanding the Obama-era Manufacturing USA Institutes program to include three biomanufacturing centers: the National Institute for Innovation in Manufacturing Biopharmaceuticals, BioFabUSA, and BioMADE.[41] Post-COVID, the Biden Administration issued two reports in 2023 (*Bold Goals for US Biotechnology and Biomanufacturing* and *Building the Bioworkforce of the Future*) promoting policies to advance the U.S. bioeconomy.[42]

These recent developments regarding more specific messaging on actors associated with biothreats, the DoD's focus on countering these threats, and the U.S. Government's commitment to growing the U.S. bioeconomy all represent important elements of potential communications—likely received and scrutinized by potential adversaries—relevant to a U.S. BW deterrence strategy. At present, however, they are separate pieces of a potential U.S. message on deterring BW. While these statements discuss some ways and means associated with deterrence by denial or deterrence by cost imposition, they are not presented as part of a comprehensive deterrence strategy focused on BW. Similarly, while the DoD has started to publicly and directly refer to specific state actors associated with biothreats, it has not incorporated actors (or the bad actions they should avoid) together into a clear deterrence message on BW. Even allowing for the important role strategic ambiguity plays within U.S. deterrence messaging (in regard to what the U.S. does and does not communicate concerning its potential actions in response to an attack), the DoD and U.S. Government's communications on BW deterrence lack cohesiveness and clarity.

ADDITIONAL CHALLENGES

Due to the characteristics of biological pathogens, deterring BW threats also carries several additional challenges derived from characteristics of these weapons that are different from other types of weaponry (to include other forms of WMD):

- Because biological pathogens are living, adaptable organisms, BW are an offense-dominant weapon. Protecting a large population from the effects of biothreats is exceedingly difficult to the point of impossibility; such efforts can, at best, offer only a "Swiss cheese" layer of shielding.[43]
- As opposed to the detonation of a nuclear weapon by an adversary carrying out a nuclear attack, the employment of a biological agent may not be immediately apparent. Some agents have incubation periods ranging from a few hours to several weeks, complicating early efforts to detect that an attack has occurred. Although the United States, along with allies and partners, have invested in extensive deployment of biomonitoring capability globally, no single cohesive national or international biological incident monitoring system currently exists.
- Biological agents can have the ability to replicate within host organisms, meaning that the initial amount released can multiply—possibly resulting in the attack inflicting more damage than intended by the perpetrator.
- Because the effects of BW and naturally occurring pathogens share similar characteristics, adversaries may assess they can maintain "plausible deniability" should they choose to employ BW. Naturally occurring pathogens (without modification) may be weaponized, and it may not be readily apparent whether a bioincident is intentional or naturally occurring simply based on analysis of the agent. It is sometimes possible for laboratory analysis, including metagenomic sequencing and functional assays, to indicate if a pathogen was genetically modified. It may also be possible to indicate that the agent was likely produced by a perpetrator (or a select set of perpetrators) based on intelligence regarding an adversary's BW capabilities. Extensive orthogonal data about the incident and possible perpetrators, however, is required for confident attribution. This factor alone is the greatest impediment to effectively executing a deterrence by punishment strategy for BW.
- BW-related technologies and pathogens pose a high proliferation risk. In contrast to nuclear research, the international biological research community is relatively open, with research possibly applicable to BW programs available in unclassified journals. Export control and select agent lists (e.g., the Australia Group) give governments tools to reduce the chances of enabling the proliferation of BW related dual-use technologies and materials; however, these are imperfect regimes. Additionally, the increasing accessibility of certain biotechnologies, like CRISPR, coupled with assistance from Large Language Models (LLMs), could lead to increased interest in BW by state and non-state actors.
- In addition, given the secrecy surrounding Russia's and China's compliance (or lack thereof) with the BWC, coupled with the inherent challenge in quantifying the effectiveness of deterrence, it is difficult to know how either of these states may interpret U.S. deterrence communications related to deterring biothreats.

ANALYSIS

In the next phase of study, the research team held two roundtable events to explore Biothreat Deterrence more fully with experts both within and outside the USG.[44] The inaugural biothreat deterrence roundtable, held by CSWMD in February 2025, was an unclassified discussion to explore options for deterring biothreats

that go beyond the United States' deterrence by denial traditional biodefense posture. The agenda featured presentations by subject matter experts covering various aspects of biothreat deterrence and concluded with a presentation of the Center's draft biothreat deterrence framework. A primary goal was to receive input on the framework, enabling revisions for the second roundtable. An additional event objective was to facilitate engagement between members of the biodefense and strategic deterrence communities, which do not routinely interact on issues of national security.

FORENSICS AND ATTRIBUTION: BIOATTRIBUTION

At the research, a Johns Hopkins University Applied Physics Laboratory team provided an overview of the technical capabilities required to more reliably apply forensics and attribute biothreats, given advancing biotechnology capabilities in the biothreat arena. The team presented these capabilities as "Bioattribution," to capture the expanded capabilities required (i.e., not just sequencing and other technical tools, but inclusive of bioinformatics and metadata on a larger scale, as well as relevant intelligence). Needs and gaps were discussed, and their key observations and takeaway recommendations were presented to the roundtable participants as follows.

- Sampling of biological signatures, including their standards, is key, and must include traditional, emerging, and novel biological entities. Pandemic scenarios should include pathogens, toxins, and other biological results.
- Early warning is critical; potential BW attacks will likely be compounded by cyber-attacks and/or information manipulation campaigns. It is also likely that degradation of information systems will be a strategic goal of the adversary.
- Bioproduction or other synthetic biological efforts (for example, the creation of bioenergetics) represent unique potential biological signatures and/or targets.
- There is a need to bring bio-use platforms to the high side for intelligence awareness. Several global health capacity databases, which are intended to bridge gaps in awareness within the intelligence community.
- It will be critical to distinguish "signal from noise" to identify real and significant threats or novel signatures.

It is unlikely there will be a "smoking gun" when it comes to a BW attack, which can contribute to strategic surprise. The first detection of BW is more likely following human-to-human transmission. Orthogonal data is needed to create a complete picture, however, along with laboratory analysis, and include the ability to detect "false positives".

An additional challenge is that possession of a robust U.S. attribution capability does not contribute to deterrence if the adversary wants it to be known they are the perpetrators. It is possible that a bad actor may want it to be understood that it initiated a BW attack while still maintaining some degree of plausible deniability to avoid serious consequences. This is along the lines of, "We did it. You know we did it…but can you prove we did it?" Potential adversaries who accompany a BW attack with information manipulation campaigns, for example, may assess the burden of proof (given the complexity of the science involved, together with their own efforts to complicate effective communication of laboratory results) is high, primarily or solely on the United States, and so resource-intensive that it will significantly slow and/or truncate the U.S. response.

Moreover, with regard to nuclear deterrence, there are several examples of advanced non-nuclear technologies that may pose challenges to the traditional U.S. concept of nuclear/strategic stability. It might

be important to ask whether there is an analogous concept of "BW stability" and if so, what would challenge that concept and make bio-deterrence more difficult? These advanced non-nuclear technologies have one or more of the following attributes:

1) Technology that moves fast and is hard to detect;
2) Technology that affects or targets command and control;
3) Non-nuclear technology that creates escalation in wartime/conflict;
4) Technology that puts our retaliatory tools at risk.

DISCUSSION OF ADVERSARY BIOLOGICAL WEAPONS COST-BENEFIT ANALYSIS

In recognition of the vital importance of tailoring deterrence to specific BW threats and contexts, roundtable participants engaged in lengthy discussions on potential adversary cost-benefit calculus relating to BW use.

SMEs emphasized that it is important to think about adversary calculus of weighing the costs of actions related to BW—what is the price, and what is the risk it assumes? An adversary leadership's calculations on why they think using BW carries acceptable risk, and why they think they can get away with it, are important to consider. While the focus here is on the adversary's calculus of attribution and deniability regarding BW employment, this calculus could also reflect broader judgments about U.S. resolve, capabilities, or other dimensions.

Roundtable participants agreed that the more the United States can gain this wider understanding, the better Washington can ultimately develop, promulgate, and tailor a BW deterrence strategy. A broader way of thinking about this in developing deterrence strategy is to pose the question, "How could deterrence fail?", which will be useful in red teaming such strategies.

The workshop identified several specific benefits and costs potential adversaries may associate with BW:

BENEFITS:

- Interfere with U.S. ability to shape the theater to our advantage (to get into theater, establish logistics), including slowing or blocking supply chains.
- Inducing a sense of exhaustion on U.S. and allied forces due to the challenges of operating in a BW environment; including preventing people from coming to work and instilling fear in allies previously poised to help.
- The adversary, based on the capabilities of emerging biotechnology, and lack of clear U.S. deterrence message, may have reason to believe they can get away with a BW attack without consequence.
- This is exacerbated by the contemporary information environment, which is often flooded with false, manipulated, or out-of-context information, to include on bioincidents (*see below*).
- BW can make up for shortcomings in conventional capabilities (e.g., an adversary may assess developing BW is less costly than developing sophisticated advanced conventional standoff capabilities).
- BW use against a U.S. ally can complicate their decision-making processes, hampering their ability to coordinate effectively with the United States.

- An adversary may use a BW attack to give itself tactical or operational breathing room. This could occur by sparking a public health crisis (pandemic or epidemic) or causing environmental contamination.
- A competent adversarial actor would understand that an infectious BW poses a risk to spread beyond their intended area of effect.
    - If it spreads to their own forces, they have the advantage of knowing exactly what the agent is. As such, they may be willing to take this risk if they already have prophylactic or treatment options in place. (The United States and its allies and partners likely would not.)
    - Even if they take a few hundred (or thousand) casualties as collateral damage from their BW attack, this may be acceptable to a potential adversary to achieve a strategic objective. Collateral damage would be even less of a concern if the BW is simply temporarily incapacitating rather than fatal.

COSTS:

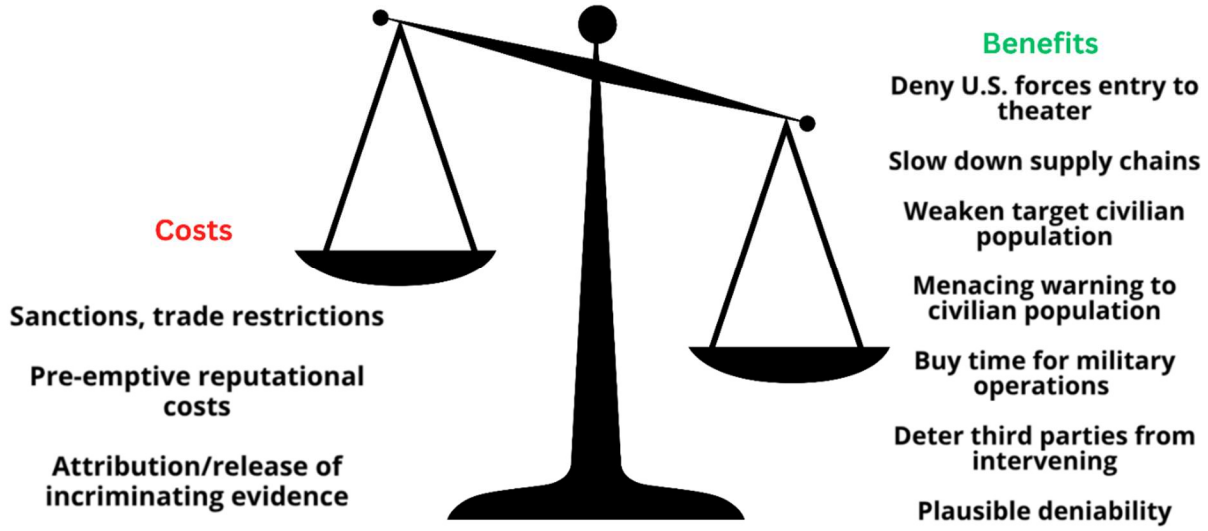
- Adversaries may not want to be seen as an international "pariah" (i.e., a potential adversary would not want to lose face; does this bad actor think they can get away with it?)

Other discussions of potential costs, however, led participating SMEs to highlight the importance of rapid changes within the biotechnology field—and how these changes may have fundamentally altered how potential adversaries assess costs traditionally associated with BW programs.

An adversary interested in BW development, for example, may conclude that advancements in biotechnology now allow it to overcome past drawbacks, such as a lack of medical countermeasures and/or potential adverse impacts to one's own force or population. While participants expressed the view that biotechnology S&T cannot eliminate potential risks and costs, they also concluded that an adversary could plausibly reach the conclusion that the present benefits of BW employment are greater than the potential costs. The lack of a well-articulated and known U.S. BW deterrence strategy also contributed to their assessment.

A key question is whether tailored deterrence includes deterring individual actors, or if it is better to attempt to deter all/any BW attacks by any actor. Participants agreed that ideally, it should be both, but the distinction might be important. There are many different people and professional disciplines that compose a BW program (scientists, funders, military, etc.). They all represent different targets for deterrence.

Figure 2. Adversary Assessment of BW: Costs and Benefits Summary



Revisiting the 4 Cs Framework

After reviewing the scenarios, participants then revisited the proposed Biothreat Deterrence Framework. Given the above consideration that an adversary, in today's landscape, may view the benefits of BW as outweighing the potential costs, a key goal for U.S. biothreat deterrence is to change this calculus (i.e., with regard to adversary views of BW programs and potential BW employment, to reduce perceived potential benefits and increase concerns about likely costs). The framework below reflects participant feedback.

Figure 3. How do we change adversary BW cost-benefit calculus?

Capabilities	Communication
Allied testing capabilities Break the MCM orientation bias against biology Demonstrate that biology can be integrated into the "big picture" Strengthen pipeline (life sciences) Break down stovepipes in education of science community	Communicate in native languages, cartoons as appropriate Private demarche through embassy Off-the-record statements by senior officials of intent/commitment to action
At what threshold does the adversary think we are going to take action?	Selectively revealing response capabilities through demonstration [note: Participants were divided on whether and how a BW deterrence strategy could be considered 'credible']
Comprehension	**Credibility**

U.S. MESSAGING AND COUNTERING ADVERSARY INFORMATION MANIPULATION

Roundtable participants asked the following questions: How should the United States message attribution, response, and retaliation? And with what level of ambiguity? In 2022, there was some very direct and clear messaging between the United States and Russia, at a very high level, concerning Russian's potential use of nuclear weapons in Ukraine, which may represent an example of the kinds of direct deterrence messaging that could be utilized in the future as part of a U.S. BW deterrence strategy.

False or manipulated information, however, can hamper the United States' ability to respond to a biothreat, or an adversary could sow distrust in U.S. medical countermeasures (MCMs) by executing an information manipulation campaign calling into question the effectiveness of the MCMs, or mislead, blaming the U.S. for an outbreak (such as China's false information to the WHO in the early investigations of COVID).

Suggested approaches to countering adversary messaging on BW include the following ideas:

- Develop a set of messages emphasizing that "we are resilient against all threats".
- There is a benefit to the use of pre-prepared narratives and issuing them rapidly. While the United States knows that it did not cause a bioincident or launch a BW attack, it must make the case with effective messaging and presentation of evidence that: a) the United States is not responsible for the BW attack, and b) also proves the adversary is the culpable party. If the United States does not have much information on the possible attack, the United States could respond with predeveloped narratives about the adversary's BW program; however, this is a zero-day exploit in that it cannot be repeated. To pre-respond in this way, the United States would need a degree of confidence that an attack is possible.
- Use private *demarche* communications.
- Use off-the-record statements by senior officials.
- Use public messaging—U.S. messaging should communicate preparedness in a digestible way for both the public and policymakers
- The United States could repeat the intelligence playbook deployed prior to the Russian invasion of Ukraine where some U.S. intelligence was downgraded and released to expose Russia's actions.
- A separate but related approach could feature sharing intelligence about a third country's BW program at the United Nations to send a message to the primary adversary that the United States knows about their program and can similarly publicly reveal this information at any time.

The use of any of these approaches will require careful thought and planning as to who is the recipient/target of such messaging, and who should deliver the message.

ROUNDTABLE DISCUSSIONS SUMMARY

With regard to deterrence tools, it may be worth developing a specific BW deterrence taxonomy organizing ("binning") the various pieces of the present U.S. toolkit for defending against biothreats.

This taxonomy could distinguish between denial and cost imposition tools. Regarding the latter, the DoD could benefit from additional assessments and guidance regarding the kinds of costs the United States is prepared to impose. It might also be useful to distinguish between tools that are material vs non-material (to include informational); kinetic vs non-kinetic; and things the United States would do on its own vs things allies can help with (to include assessments, where relevant, of changes to burden-sharing). Tools should

probably include declaratory policy, broadly defined, which could include such statements on BW deterrence similar to U.S. nuclear declaratory policy statements within past NPRs, as well as additional public statements designed to shape adversary perceptions of potential costs associated with their development or employment of BW.

Deterrence tools:

- Deterring BW development earlier (in "peacetime") is a key goal, along with a standard toolkit, as opposed to "ad hoc" courses of action applied only in crises or conflicts. It also may be valuable to exercise against certain BW employment scenarios during peacetime.
- Knowing the potential adversaries' decision calculus, including the question of their BW 'doctrine'. (For a VEO that might be a senior leader and their interest in BW.)
- Use strategies to taint the reputations of known BW weaponeers.
- Invest in biosensors to speed detection (including advanced emerging biotechnologies).
- Perform capability exercises, i.e. "Exercising the attribution muscle" for regular, everyday biological events.
- Do a public-facing demonstration of such a capability exercise (demonstrate excellence in forensics and attribution).
- Use BWC mechanisms (multilateral) where a compelling narrative is used to do attribution; Article 6, despite caveats, is available as a tool.
- Utilize the UN Secretary General mechanism—this can allow for investigations which, outside of determination of findings, can serve to *disrupt* ongoing BW programs. Those investigated may be forced to displace key individuals, enact rapid shifts in expenditures, or move the program out of a building, etc.
- Signal that the United States has a particular capability that would deter (to include consideration of signaling regarding capabilities presently under development).
- Selectively reveal an existing capability.
- If the United States does not have much info on the possible attack, the United States could respond with predeveloped narratives about the adversary's BW program; however, this is a "0" day exploit that cannot be repeated.

How do we know our deterrence efforts are impactful?

- An actor changes their diplomatic approach (opens or engages in dialogues); including changes in behavior at the BWC.
- Observed changes by intelligence; including an overall change in an adversary's approach to BW development over time.
- Legal actions are initiated by the adversary.
- Changes in frequency or type of adversary information manipulation campaigns featuring or including references to BW or BW-related topics.
- Changes in a potential adversary's strategies for the bioeconomy, including changes in investment posture in bioeconomy or biotech/related tech.

Use of international forums

- The fact that adversaries may be part of the BWC enables the United States to possibly call into question their compliance.
- The UN Secretary General's consultative mechanism may be leveraged to investigate an adversary.
- A WHO investigation could be used as well; this may not fully unravel an adversary's BW program, but it could certainly slow it down by shining a spotlight on their activities.

REFERENCES

[1] Dr. Seth Carus, personal interview, 17 January 2025.

[2] DoD, *2023 Biodefense Posture Review* (DoD: Washington D.C., August 2023), https://media.defense.gov/2023/Aug/17/2003282337/-1/-1/1/2023_BIODEFENSE_POSTURE_REVIEW.PDF, 1.

[3] DoD, *Deterrence Operations Joint Operating Concept,* version 2.0 (DoD: Washington D.C., December 2006), 3, 26–27.

[4] Ibid., 5.

[5] Jonathan B. Tucker and Erin R. Mahan, *President Nixon's Decision to Renounce the U.S. Offensive Biological Weapons Program*, NDU Center for the Study of WMD Case Study #1 (Washington D.C.: NDU Press, October 2009)

[6] Michael R. Fraser, Raphael M. Barishansky, and James S. Blumenstock, "Twenty Years After 9/11: The Public Health Preparedness We Need Now," *American Journal of Public Health*, 111(9), 1562–1564, 2021, https://doi.org/10.2105/AJPH.2021.306459.

[7] Library of Congress, "Federal Efforts to Address the Threat of Bioterrorism: Selected Issues and Options for Congress," by Frank Grotton and Dana A. Shea, updated 8 February 2011, https://crsreports.congress.gov/product/pdf/R/R41123, 4, 9–13.

[8] Ibid., 4.

[9] Department of Defense, *Biodefense Posture Review* (Washington D.C.: Department of Defense, August 2003).

[10] National Biodefense Strategy and Implementation Plan, (created in 2018, updated in 2022). https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf

[11] White House Security Memorandum 15, 2022. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/10/18/national-security-memorandum-on-countering-biological-threats-enhancing-pandemic-preparedness-and-achieving-global-health-security

[12] Tech Sergeant Nicholas Perez, 151st Wing, "Air Guard Deploys for Toxic Swell Joint Training Exercise," National Guard press release, 28 August 2024.

[13] U.S. Embassy in the Philippines, "U.S., Philippines Inaugurate Training Center for Biological and Chemical Security Response," U.S. Embassy press release, 23 February 2024.

[14] Nist Bioeconomy Lexicon defining Biosecurity. https://www.nist.gov/bioscience/nist-bioeconomy-lexicon

[15] DoD, *Nuclear Posture Review* (Washington, D.C.: DoD, December 2022): 8.

[16] George H.W. Bush, "Text of Bush's Letter to Saddam Hussein," *LA Times*, 13 January 1991. https://www.latimes.com/archives/la-xpm-1991-01-13-mn-412-story.html.

[17] James A. Baker, III, with Thomas M. DeFrank, *The Politics of Diplomacy: Revolution, War, and Peace, 1989-1992* (New York: G.P Putnam's Sons, 1995), p. 359.

[18] Department of Defense, "Briefing by Secretary Mattis on U.S. Strikes in Syria," briefing transcript, 13 April 2018. At the briefing, Secretary of Defense Mattis noted deterring future chemical weapons attacks was a key purpose of the strikes: "French, British and U.S. forces struck targets in Syria in support of President Trump's objective to deter the future use of chemical weapons".

[19] Raymond A. Zilinskas, *The Soviet Biological Weapons Program and Its Legacy in Today's Russia*, Center for the Study of Weapons of Mass Destruction, Occasional Paper 11, Washington DC: National Defense University Press, July 2016, https://wmdcenter.ndu.edu/Portals/68/Documents/occasional/cswmd/CSWMD_OccasionalPaper-11.pdf?ver=2016-07-18-144946-743, 12-13.

[20] Zilinskas, *The Soviet Biological Weapons Program and Its Legacy in Today's Russia*, 12, 44-45.

[21] Department of State, "The Kremlin's Never-Ending Attempt to Spread Disinformation about Biological Weapons," Global Engagement Center, March 14, 2023, https://2021-2025.state.gov/the-kremlins-never-ending-attempt-to-spread-disinformation-about-biological-weapons/.

[22] "Russia to continue probing into activities of US biolabs worldwide—senior MP," *TASS*, 18 August 2023, https://tass.com/russia/1662425.

[23] Gigi Kwik Gronvall and Aurelia Attal-Juncqua, "Assessing the Trajectory of Biological Research and Development in the Russian Federation," Joint Force Quarterly 108, National Defense University Press, January 16, 2023, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3262779/assessing-the-trajectory-of-biological-research-and-development-in-the-russian/.

[24] Department of State, *Adherence to, and Compliance with, Arms Control, Nonproliferation, and Disarmament Agreements and Commitment* (Department of State: Washington D.C., April 2024): 26.

[25] Patrick Beyrer, "Taking Stock of U.S.-China Biotechnology Competition," Asia Society Policy Institute, May 15, 2024, https://asiasociety.org/policy-institute/taking-stock-us-china-biotechnology-competition.

[26] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (5 February 2024): 10.

[27] Department of Defense, *Military and Security Developments Involving the People's Republic of China*, 2024 (Washington D.C.: Department of Defense, December 2024): 111.

[28] Elsa B. Kania, "Designing Deterrence: The PLA's Outlook on Disruptive Technologies and Emerging Capabilities," in *Modernizing Deterrence: How China Coerces, Compels, and Deters*, ed. Roy D. Kamphausen, National Bureau of Asian Research, 2023, https://www.nbr.org/wp-content/uploads/pdfs/publications/modernizing-deterrence_feb2023.pdf, 127-128.

[29] Kania, "Designing Deterrence: The PLA's Outlook on Disruptive Technologies and Emerging Capabilities," 120, 122.

[30] Emily Harding and J. Stephen Morrison, "Biodefense Posture Review Raises Alarms about New Threats but Speaks Softly on China," Center for Strategic and International Studies, August 23, 2023, https://www.csis.org/analysis/biodefense-posture-review-raises-alarms-about-new-threats-speaks-softly-china.

[31] Patrick Tucker, "As DOD steps up response to bioweapon threat, China plays complicated role in biosecurity," Defense One, August 24, 2023, https://www.defenseone.com/technology/2023/08/dod-steps-response-bioweapon-threat-china-plays-complicated-role-biosecurity/389714/.

[32] Mr. Paul Bernstein, personal interview, January 22, 2025.

[33] Dr. Seth Carus, personal interview, January 17, 2025.

[34] Council on Strategic Risks, "Expert Reactions to the Updated U.S. Biodefense Strategy and Implementation Steps," Nolan Center, October 18, 2022, https://councilonstrategicrisks.org/2022/10/18/expert-reactions-to-the-updated-u-s-biodefense-strategy-and-implementation-steps/.

[35] DoD, "Strategy for Countering Weapons of Mass Destruction," 2023, https://media.defense.gov/2023/Sep/28/2003310413/-1/-1/1/2023_STRATEGY_FOR_COUNTERING_WEAPONS_OF_MASS_DESTRUCTION.PDF, VII.

[36] DoD, "Chemical and Biological Defense Program Enterprise Strategy 2024," Office of the Deputy Assistant Secretary of Defense for Chemical and Biological Defense," https://media.defense.gov/2024/Dec/18/2003615893/-1/-1/0/CHEMICAL-AND-BIOLOGICAL-DEFENSE-PROGRAM-ENTERPRISE-STRATEGY-2024.PDF, 5.

[37] DoD, "Strategy for Countering Weapons of Mass Destruction," 2023, 1; U.S. Department of Defense, "Chemical and Biological Defense Program Enterprise Strategy 2024," 5.

[38] DoD, "Strategy for Countering Weapons of Mass Destruction," 2023, 1; U.S. Department of Defense, "Chemical and Biological Defense Program Enterprise Strategy 2024," 5.

[39] Mr. Paul Bernstein, personal interview, January 22, 2025.

[40] Shannon Green, Nathan J. Hillson, John Moulton, Harshini Mukundan, Daniel P. Regan, Deepti Tanjore, "A Biomanufacturing Plan to Confront Future Biological Threats," Council on Strategic Risks, September 2024, https://councilonstrategicrisks.org/wp-content/uploads/2024/09/BiomanufacturingPlan-1.pdf, and

U.S. Library of Congress, "The Bioeconomy: A Primer," by Marcy E. Gallo, updated September 19, 2022, https://crsreports.congress.gov/product/pdf/R/R46881, 7–8.

[41] Green et al, "A Biomanufacturing Plan to Confront Future Biological Threats," 8.

[42] Green et al, "A Biomanufacturing Plan to Confront Future Biological Threats," 8–9.

[43] Dr. Seth Carus, personal interview, January 17, 2025.

[44] The roundtable had 32 participants, including 10 speakers and moderators. Participants represented 18 different organizations, including the Centers for Disease Control and Prevention, Department of Commerce, Department of Homeland Security, Department of State, National Academies, NationalSecurity Council, Federal Bureau of Investigation, Office of the Director of National Intelligence, Pacific Northwest National Laboratory, Atlantic Council, and RAND Corporation. See roundtable report for details.

Appendix 1: Notional Scenarios Used for Guided Discussion

As a component of the April 23rd follow-on workshop, three notional scenarios were presented in a guided discussion session to roundtable participants to think through how the draft biothreat deterrence framework may function in different crisis contexts. The discussion generated by these outcomes informed the overall findings as noted in the study.

The scenarios discussed were intended to stimulate discussion on deterrence ideas, tools, and options. Two scenarios were used, one to examine BW use in conflict by a State actor, and one to examine VEO use.

Scenario 1: *Shaping the Battlefield* (infectious agent released by a state actor, accompanied by an information campaign).

- "Muddy the waters," distract, get something else in headlines
- Prevent the United States from shaping the theater
- Compromise defensive combat operations
- Exhaust Blue defenders as a way to enable Red force
- Red may perceive biological weapons as their "overmatch" zone
- Deterrence of Blue/Green
- Create combat pause under humanitarian pretense
- Red may perceive that the United States will not intervene or at least won't be able to attribute the bio attack.

What is the U.S. deterrence toolkit for this notional scenario?

- Minimal passive defenses for USAF bases, none for most others.
- United States would be challenged to gain control of the information environment. Lessons learned from Ukraine?
- Best defense is building deterrence in peacetime—holding exercises, conducting pilots of at-home test kits, exercising attribution

Scenario 2: *Bioterrorism* (non-infectious toxin attack on CONUS by a violent extremist organization). Possible adversary cost-benefit calculus:

- Diminish support for Country B (U.S. is supporting a besieged country)
- Punish supporters of Country B
- Show how powerful the VEO is
- Cause fear and terror; "Warning shot"

What is the U.S. deterrence toolkit for this notional scenario?

- Law enforcement could take action to dismantle VEO
- Intermittent punishment by U.S. can reinforce deterrence credibility

For any questions or comments about the report, please contact
DTRA: DTRA-OB-INA@groups.mail.mil