VIRAL PANDEMIC PATHOGENS FOR COVERT CONFLICT IN THE GRAY ZONE: THE NEXT GENERATION OF BIOLOGICAL WEAPONS?

NICHOLAS F. MARKO, MD, FAANS, FACS

INTRODUCTION

Biological weapons (BW) were historically envisioned as adjuncts to kinetic warfare intended for deployment in battlefield scenarios and targeted against enemy combatants[1]. Under this paradigm, efforts were made during and after World War II to develop ballistic delivery methods for biological agents, to weaponize microorganisms such that their pathogenic potential was preserved during battlefield delivery, to increase the virulence of the pathogens in order to minimize the quantity of agents necessary for delivery, and to develop deployment strategies designed to maximize enemy casualties and minimize collateral damage[1-5]. Ratification of the Biological Weapons Convention (BWC) in 1975[6] and the fall of the Soviet Union in 1991[7] catalyzed the end of most state-sponsored BW development efforts, and possible scenarios for their application shifted away from large-scale battlefield employments against enemy armies toward smaller-scale, more covert use by non-state actors as instruments of terror[1]. More recently, advances in biotechnology[8] and proliferation of high-containment laboratories[9] have raised concerns about accidental releases of genetically-modified pathogens into civilian populations[10], while fears regarding climate change[11] and globalization[12] have increased the interest in naturally-occurring pandemics. As a result, the majority of current biodefense and biosecurity efforts are focused either on bioterrorism prevention and preparedness, on managing spontaneous disease outbreaks, or on improving global biosafety[13-16].

This analysis focuses on a different biological risk scenario that has heretofore received relatively little attention in the academic literature. Specifically, it examines how the evolving nature of modern warfare and warfighting objectives, changing social conditions and dynamics on a global scale, and rapid advancements in biotechnology have combined to create a novel niche for a potential, new approach to biological warfare by state actors. The proposed scenario involves the covert use of modified or unmodified viral pathogens of pandemic potential ("pandemic biological weapons") by state actors against civilian populations in order to achieve a global, strategic advantage. The characteristics of the pathogen and the scale of its deployment could be tailored to meet the specific objectives of the aggressor, and strategic advantage would be achieved through subsequent manipulation of the large-scale, asymmetric economic disruption and social destabilization associated with the ensuing regional or global pandemic.

The potential viability of this strategy will be investigated through a discussion that is structured in six sections. The first section will present a brief overview of the changing nature of geopolitical conflict and its effects on concepts of warfare and conflict in the modern era. This will culminate in a discussion of how the changing nature of conflict opens the door for a new generation of biological weapons. Section two will describe prior factors that have historically mitigated the use of biological weapons by state actors and will highlight the fading relevance of these factors in the modern era. It will then contrast these with the potential, unique advantages associated with covert use of viral pandemic pathogens as weapons in the new area of gray zone warfare. Section three will focus on the technical feasibility of the proposed approach by enumerating the features of the modern social and technical environments that might facilitate the proposed BW utilization scenario. Section four will present a unique spin on the "lessons learned" trope, examining the COVID-19 experience from the perspective of a potential state user of pandemic bioweapons targeted covertly at civilians. Section five will discuss the operational elements of a proposed scenario for covert, state use of a pandemic biological weapon on a global scale, including planning, preparation, execution, and modulation phases, in order to demonstrate its general feasibility. Finally, section six will discuss selected counterarguments against the proposed scenario and will consider their merits and flaws. Together, these discussions will illustrate that deliberate, covert application of viral pandemic biological weapons by state actors as a form of gray zone warfare may be both feasible and practically achievable in the modern era.

SECTION 1: OPENING THE DOOR: THE CHANGING NATURE OF WARFARE

At its most basic level, the fundamental nature of warfare remained unchanged throughout thousands of years of human history. Warfighting historically involved direct confrontation by combatants and the use of lethal force. When conducted at scale, the warring parties were generally represented by soldiers, organized into armies fighting on behalf of a state. While the weapons, tactics, motivations, and nature of the combatants has evolved over time, warfare adhered to this "kinetic" model of conflict resolution well into the 20th century. Kinetic conflict is still a major focus of state militaries, and modern approaches to these ends are a mainstay of international conflict[17, 18].

The long history of kinetic combat notwithstanding, scholars of warfare have recognized for centuries that war is an extension of politics[19]. This theme is prevalent in literature on the philosophy of warfare, from Sun Tzu's discussions of the interconnectedness between diplomacy, economics and warfare[20], to Von Clausewitz's characterization of war as, "policy by other means.[21]" In this context,

and catalyzed by the recent acceleration of globalization and the rapid progress of technology, both state- and non-state combatants have increasingly begun to explore "non-kinetic" methods of warfare as a means of achieving sociopolitical objectives outside of the confines of the traditional battlefield. This approach pays heed to the wisdom of Sun Tzu, who noted that, "to subdue the enemy without fighting is the acme of skill.[20]"

The changing nature of warfare has been acknowledged by state militaries across the globe. In the doctrinal military publication, *The Science of Military Strategy*, strategists from China's People's Liberation Army noted as early as 1999 that, "the boundaries lying between the two worlds of war and non-war, of military and non-military, will be totally destroyed," and that, "the rules of war may need to be rewritten," as we enter a time where, "soldiers no longer have a monopoly on war.[22]" American military strategists have similarly recognized the evolving nature of conflict by noting the rise of what they term, "Irregular Warfare (IW)." The US Department of Defense describes IW as, "a struggle among state and non-state actors to influence populations and affect legitimacy," and notes that, "IW favors indirect asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will.[23]" This explanation highlights that there are both kinetic and non-kinetic means of conducting IW, but the objective of both approaches is to compromise the power, will, and legitimacy[24, 25] of the opponent rather than to inflict direct damage to infrastructure or to cause casualties through force. While US and Chinese doctrine have some specific differences in these areas[26], and while semantic arguments regarding precise definitions persist[27, 28], it is clear that major world powers recognize that the goals and objectives of warfare are evolving and that tactics must evolve in order to keep pace.

Two, related concepts that are salient to the present discussion are, "asymmetric warfare (AW)," and, "hybrid warfare (HW)." Asymmetric warfare is described as, "a type of war between opposing forces that have divergent military power, strategy, or tactics," and that, "often involves the use of unconventional weapons and tactics.[29]" This highlights the value of IW operations specifically when there is a mismatch between opponents in conventional warfare capabilities. Related but distinct, the concept of hybrid warfare derives from the observations that modern adversaries can combine military and nonmilitary tools and tactics to, "overwhelm through complexity," and that opponents employing such tactics often cannot be defeated, "in 'Clausewitzian' terms, through a conventional military campaign culminating in a decisive battle.[30]" Russian Chief of the General Staff Valery Gerasimov has extolled the value of such tactics[31], and they were employed successfully in the Russian annexation of Crimea in 2014[30].

Together these evolving concepts of warfare (IW, AW, HW) give rise to a new battle space, which some refer to as the, "gray zone.[18, 32-35]" Broadly speaking, the gray zone has been described as, "the space between war and peace.[36]" It is, "characterized by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war.[32]" Conflict, variably referred to as "competition[37]" or as "warfare[32]" in the gray zone, "has increasingly been the strategy selected by states that are determined to influence change without the risk of major escalation to outright military war.[38]" Gray zone tactics, which are said to avoid, "both the risks of war and the rules of peace,[18]" often involve, "small-footprint, low-visibility operations often of a covert or clandestine nature,[32]" and leverage, "non-official or plausibly deniable proxies…deniable forces, and disinformation campaigns.[39]" As large-scale, international, kinetic operations become less palatable and less winnable, the gray zone is emerging as a critical battle space in modern geopolitical conflict.

The degree and the nature of the overlap between IW, AW, and HW, as well as their specific relationships to "gray zone operations," continue to be debated in the military community[25], but the accelerating cadence with which these issues are discussed prompts several, important conclusions. First, semantics aside, the evolving nature of modern warfare and the importance of unconventional weapons and tactics is broadly recognized across the world. Second, adopting IW-type strategies into comprehensive military operations and developing methods for countering their employment by opponents is considered a priority by the US[23, 32, 38, 39], Chinese[22, 37, 40], and Russian[18, 31, 41] militaries, which represent the current, dominant world military powers. Third, the specific value of non-kinetic methods of conducting unconventional or irregular warfare is becoming progressively more apparent as direct, military combat yields prominence to less conspicuous methods of global, geopolitical conflict[25, 30, 32, 37, 38]. Fourth, hybrid approaches to asymmetric, irregular warfare bolster the relevance of states with less extensive conventional forces and present an avenue through which they can achieve a degree of global influence that is disproportionate to their conventional military power [30, 42]. Finally, the gray zone is emerging as the new battlefield, on which world powers compete for dominance and influence alongside smaller states by manipulating the social, economic, and political environments of their adversaries[32, 38, 40, 41].

SECTION 2: BIOLOGICAL WEAPONS, THEN AND NOW

Historical Mitigating Factors to BW Use. From the post-WWII era to the end of large-scale, state-sponsored BW programs in the 1970s-1990s, biological weapons were primarily conceptualized as one type of armament that could be used in a traditional, kinetic warfighting scenario[5, 43-46]. Operating under this paradigm gave rise to several operational and technical constraints that limited their utility and rendered them generally inferior to conventional and nuclear weapons. First, selection of appropriate pathogens for weaponization was inherently limited by the scientific knowledge and available technologies. Bacteria were the best understood pathogens of the day, and laboratory materials and techniques for their manipulation were the most robust. Countermeasures were also available for prevention and treatment of collateral casualties, and so bacterial BW dominated the research and development (R&D) space[5, 43]. This restricted the potential use of viral BW to a few, fastidious organisms (e.g. smallpox), rendering inaccessible many of the potential advantages that viral BW might afford. Second, battlefield munitions capable of effective, uniform deployment of weaponized biological agents needed to be developed. This was a major challenge in the early days of state-sponsored BW programs[4, 47]. Extensive military R&D solved this issue over the ensuing decades[43, 48], but effective delivery by smaller states and non-state actors remained a persistent challenge that mitigated widespread use of traditional BW agents. Third, the process of "weaponizing" pathogens to make them stable under the conditions of prolonged storage and battlefield deployment was not trivial. Effective strategies were developed for some agents, but these required niche expertise, extensive laboratory and production resources, careful quality control, and considerable funding[5, 43, 49]. Fourth, secrecy was paramount for most of this research, and many R&D programs were also conducted covertly. Covert operations, in particular, slow the R&D process, limit the influx of novel ideas, constrain information sharing between experts, and complicate production logistics[49]. Finally, organizational factors, challenges with project management, and effective transfer of tacit knowledge further contributed to the challenges associated with fielding effective BW military capabilities[49]. These challenges proved particularly detrimental to BW proliferation and use when contrasted with the relative ease of development and production, the overall stability and predictability, and the demonstrated efficacy of conventional and nuclear weapons[50]. Together, these factors combined to relegate BW to a trivial role in large-scale, kinetic warfare by major world powers and to render them practically inaccessible to smaller states and non-state actors. In short, the technical and practical limitations associated with traditional BW meant that they were never able to find an effective niche that was not better filled by an alternate weapons technology.

A Niche Emerges. Traditional BW failed to find a unique niche in conventional, kinetic warfare, and this combined with their unique challenges[50] and social taboo to limit their military value and utility[51]. However, Section 1 of this discussion has outlined the emergence of a potential new niche attributable to the evolving world of non-kinetic, irregular warfare. This creates demand for a new type of weapon that is uniquely suited to covert action in gray zone conflicts. While conventional and nuclear munitions may retain utility in kinetic scenarios, they are inherently incapable of completely filling this covert niche. In this context, a potential role for novel BW agents emerges.

Several features of gray zone warfare suggest potential value for BW agents. First, the primary objectives of this type of conflict are neither material destruction nor immediate lethality, which are the principal purview of conventional and nuclear weapons. Instead, gray zone warfare objectives involve compromising the economy and social fabric of an enemy, undermining cohesion among its citizens, degrading its legitimacy on the world stage, and degrading the will of its citizens to stand together and fight[25, 32, 37, 38, 40, 41]. The recent COVID-19 pandemic has illustrated how pandemics can affect all of these features of a society, and the mechanism for catalyzing a deliberate pandemic would be the use of a pandemic biological weapon. Second, considerable importance in gray zone conflict is placed on plausible deniability and lack of effective attribution[33-35, 52]. The COVID-19 pandemic has also illustrated the challenges associated with biological attribution, a lesson that could be leveraged to the advantage of a gray zone aggressor. Accordingly, Section 3 of this analysis will examine specific lessons learned from the pandemic that support the disruptive potential of an engineered pandemic. Based on analysis of the recent pandemic experience, an argument will be made in support of the potential value of BW in modern, gray zone warfare.

The emergence of a novel niche, however, is only one part of the equation. In order for a BW agent to fill this niche, its mechanism of action on the target population must be consistent with its intended socioeconomic objectives. Historical BW are poorly suited to this task, as they were optimized for use on the battlefields of a kinetic war. Kinetic shelling with BW munitions is both overt and attributable, and its effects, when used to deliver bacterial pathogens optimized for infection via direct exposure, are limited to the specific geographic area of attack. Additionally, effective countermeasures are currently available against nearly all previously weaponized pathogens[53]. Together, the limited geographic effects and the availability of effective treatments would prevent the type of widespread, self-sustaining transmission that would be required to catalyze a pandemic capable of compromising enemy economies, social structures, and morale.

These arguments suggest that a novel type of BW agent is necessary for effective use as a weapon of irregular, gray zone warfare. Specifically, the agent must not be attributable to the aggressor, the epidemic that it causes must be self-sustaining, and the available medical countermeasures must be limited. Beyond this, the balance between the nature of symptoms and the morbidity and mortality of the disease can be tailored to strategic needs either by selecting appropriate, natural pathogens or by engineering novel pathogen variants through genetic manipulation.

In order for a BW agent to fill the emerging niche, two requisite criteria must be met. First, it must be technically possible to engineer such a weapon using current technologies. Section 4 of this analysis will, therefore, examine the current technological facilitators for constructing BW agents intended for use in gray zone warfare. Second, a strategy for deployment of the weapon consistent with the principles of gray zone warfare must be developed. Section 5 of this analysis will present one example of such a deployment scenario. Together, sections 3-5 will solidify the argument for the potential viability of pandemic biological weapons as novel agents of gray zone warfare.

Section 3: COVID-19: Lessons Learned for Biological Warfare in the Gray Zone

Introduction. Recognizing the emergence of a niche for novel weapons of gray zone warfare, an aggressor will consider a wide variety of potential weapons to facilitate competition in this space. The recent COVID-19 pandemic offers several, significant lessons that would lend credence to the consideration of pandemic biological weapons as a potential path to covert dominance. This section will discuss four such lessons learned from the COVID-19 pandemic and their utility to the gray zone aggressor.

Lesson 1: Pandemics can cause significant social destabilization. As with previous pandemics[54, 55], COVID-19 had obvious destabilizing effects on multiple societal domains[56]. Careful observation reveals significant overlap between these effects and the intended outcomes of gray zone warfare. First, the COVID-19 pandemic demonstrated the potential for such events to sew political discord. Studies show that "pandemic fatigue" has been linked to individual-level discontent by citizens with their government, manifesting as governmental distrust, protests, and propagation of "conspiracy theories.[57]" Data also demonstrates a direct correlation between citizens' perception of the efficacy of pandemic response and their overall trust in their government[58]. This is particularly significant, as research has demonstrated that public mistrust is associated with diminished government legitimacy[59] and that, "a climate of mistrust has significant consequences on the government's ability to deliver on policies and [to] enforce

the law.[58]" Additional research has demonstrated that public mistrust of government correlates with election fraud beliefs, antigovernment protests, political extremism, and the willingness to use violence to achieve political aims[58, 60, 61]. Increasing violence tends to reinforce governmental distrust[58], thus contributing to a vicious cycle of social unrest, and, during the one-year period from 2020-2021 (during the height of the COVID-19 pandemic), the rates of violent crime and hate crimes rose dramatically in the United States[58]. The net result of all of these effects is internal political conflict and domestic political destabilization[62].

Political trust and legitimacy are not the only social dimensions strained by pandemics. Data from England, for example, suggests that, "overall levels of social cohesion are lower in June 2020 compared to all of the examined pre-pandemic periods," and that, "the decline of perceived-cohesion is particularly high in the most deprived communities, among certain ethnic minority groups and among the lower-skilled.[63]" Several studies of self-reported data regarding interpersonal relationships demonstrate perceived adverse effects of the pandemic on such relationships[64, 65]. The nature of interpersonal relationships was also affected, including, "dramatic change to social interaction necessitated by efforts to control the spread of COVID-19," in social networks, social support, social and interactional norms, and intimacy[66]. Feelings of loneliness, vulnerability, and emotional distress also increased in prevalence during the COVID-19 pandemic[67]. Interpersonal trust was similarly adversely affected, although in a less predictable fashion[68]. Childhood education also suffered, with learning losses and falling test scores observed across all grade levels[69, 70] during and after the height of the pandemic. This has been attributed to a combination of declining school enrollment, severe staff shortages, reduced instructional time, increased reliance on remote learning models, higher rates of mental health challenges, and increased misbehavior and violence in schools[71]. Rebound from these losses remains slow, suggesting that long-term adverse educational consequences may be associated with pandemics[71, 72]. Taken together, these findings suggest not only that pandemic periods adversely affect both the psychosocial condition of individuals and the nature of their social interactions with each other, but also that they create an educational deficit among children that may take considerable time and effort for a society to correct.

Political and social destabilization are explicit objectives of gray zone warfare, and the COVID-19 experience has demonstrated that pandemics precipitate both. A gray zone aggressor can glean from these findings that pandemics may be effective agents for disrupting social cohesion and destabilizing the social and political domains of enemy societies.

Lesson 2: Pandemics have significant economic consequences. The global economic consequences of the COVID-19 pandemic were myriad and substantial. A steep stock market decline from 20 February – 7 April, 2020[73] marked the onset of a global recession that persisted at least until the end of the calendar year[74]. This was associated with rising unemployment, global supply chain disruptions, food and energy crises, and a global microchip shortage, resulting in a 7-8% drop in global commerce in 2020[75]. The US economy shrank by 3.5%[76], and the EU's GDP fell by 6%[77]. The distribution of economic effects varied by sector, with those relying on physical presence experiencing the most significant losses[78]. Business closures increased precipitously[79], leading to job losses[80] and global increases in unemployment[81]. These adverse economic effects necessitated the creation of government assistance programs for businesses and individuals[82]. As acute economic downturns stabilized and reversed over the following two years, an inflation surge developed[83], and global economic growth again slowed[84].

This is a very brief summary of the economic consequences of the COVID-19 pandemic, and considerably more detail is available elsewhere[56, 85, 86]. This high-level discussion is intended to illustrate the profound economic effects of a global pandemic, because economic decline and political instability are linked[87-90]. In gray zone warfare, economic disruption of an enemy is, therefore, both an end unto itself and a mechanism for catalyzing political instability. Therefore, the COVID-19 experience clearly demonstrates the potential for pandemics to significantly compromise and destabilize the global economy.

Lesson 3: Even in the modern era, the spread of a viral pandemic cannot be interrupted in a timely fashion. The previous discussion, as well as a historical review of epidemics and pandemics, suggest the potential for significant social, cultural, and economic disruption associated with these events[54, 55]. However, until the global experience with COVID-19, an aggressor may have had reservations regarding the degree to which such destabilization could be realized from similar events in the modern era. Since the influenza pandemic of 1918, dramatic advances in biomedical science have transpired, and considerable investments have been made in public health infrastructure[91]. In theory, this could suggest that viral pandemics in the modern era would be easier to mitigate and less impactful to society. Unfortunately, the COVID-19 pandemic provided first-hand evidence that our ability to interrupt the evolution of an airborne or droplet-borne viral pandemic in the modern era remains limited. While more rapid vaccine development[92] and improved sanitation practices[93] relative to the previous century undoubtedly helped to mitigate the overall impact of the COVID-19 pandemic, the magnitude of its global

consequences cannot be denied. Moreover, it was ultimately a combination of simple public health practices (hand washing, masking, and judicious use of quarantine)[94, 95] and (perhaps) an eventual increase in population immunity[96] that brought about the end of the pandemic phase of COVID-19[97]. This reduction in prevalence and severity, however, took more than three years to transpire[98]. This experience teaches a gray zone aggressor that the evolution of at least some viral pandemics still cannot be rapidly interrupted, thus affording adequate time for the socioeconomic consequences of these events to be realized, manipulated, and exploited.

Lesson 4: Forensic microbial attribution remains difficult. The current debate regarding the origins of the COVID-19 pandemic[99-102] illustrates the difficulty associated with definitive attribution of the proximate origin of a viral pandemic pathogen. A recent report by the RAND Corporation highlights this challenge, noting that, "[i]nvestigating and attributing biological incidents can present additional complexities in detection and confirming a deliberative versus natural event. Even four years after the coronavirus disease 2019 pandemic, the U.S. Intelligence Community has differing assessments on its origins.[103]" Pathogen attribution problems derive from several challenges. First, generating reliable scientific data for attribution is non-trivial. These efforts fall within the purview of microbial forensics[104-106], a nascent science with an unproven track record. While evolving laboratory methods (e.g. next-generation sequencing) promise to improve the accuracy of molecular attribution[104], the largely-unproven nature of the discipline opens the door to challenges of the legitimacy of the data that it produces. Second, the BWC has notoriously weak investigative and enforcement provisions, and no international agency currently serves as a repository of materials or expertise focused on biological attribution[6, 107, 108]. This implies that attribution investigations would likely be conducted by individual states, a situation that opens the door to challenges based on ulterior political motives. These circumstances cultivate plausible deniability, even in the presence of objective data. Third, lists of "red flags" that suggest that a biological incident is deliberate are widely publicized[103], and these could be used as a partial roadmap for successful obfuscation of a BW attack by its planners. Fourth, accurate attribution often requires access by investigators to reference samples and associated data, which could be selectively withheld or compromised by a covert aggressor[109]. Finally, there may be few or no molecular features capable of distinguishing a BW agent from either a natural variant or a laboratory sample. This circumstance can be exploited during pathogen selection or engineering by the bioweaponeer. Accordingly, the known challenges associated with molecular attribution of pandemic pathogens, combined with the practical example of contested attribution of the origins of the Sars-CoV-2

virus, highlight for the gray zone aggressor the potential for plausible deniability associated with deliberate use of pandemic pathogen weapons.

Summary. Discussions of "lessons learned" from the COVID-19 pandemic typically focus on strategies for improving public health or policy issues related to preparedness, prevention, or response[110-112]. Unfortunately, the same pandemic offers valuable lessons to a gray zone aggressor considering viral pandemic pathogens as potential, novel weapons in their arsenal. In this context, the global experience with the COVID-19 pandemic has highlighted several potentially attractive features of such agents. It has demonstrated that, despite years of preparation, there are no effective strategies for promptly disrupting the progression of pandemics catalyzed by appropriately selected viral pathogens. Future global responses to such events may take months to years to bring the pandemic under control, and this provides adequate time for the disruptive effects of the aggression to unfold. Regarding these effects, the COVID-19 pandemic has illustrated that the consequences of such events extend far beyond the direct morbidity and mortality that they cause for individual victims. The social and economic consequences of a pandemic can destabilize the fabric of nations, and the downstream effects can persist for years after the acute event has concluded. This type of destabilization is the principal goal of gray zone operations, and few other weapons afford the promise of such prompt and wide-reaching disruption at scale. Finally, the COVID-19 pandemic has illustrated the difficulties associated with definitive attribution of pandemic pathogens and has highlighted the many points in an investigation at which plausible deniability can be introduced and maintained by an attacker. Such deniability is a necessary feature of a covert, gray zone weapon, and it is a potential advantage of using pandemic pathogens to these ends. The recent, global experience with the COVID-19 pandemic has, therefore, suggested the potential utility of viral pandemic pathogens as novel weapons of gray zone warfare.

SECTION 4: MODERN FACILITATORS OF GRAY ZONE BIOLOGICAL WARFARE

Introduction. The first generation of BW (approximately 1920-1990) failed to find a practical context for employment because of factors falling broadly into one of three categories. First, there were significant technical challenges to developing BW that could be used successfully in kinetic warfare. R&D efforts throughout this time period ultimately addressed this challenge, but it took considerable time and effort to achieve. Second, by the end of this time period, technical advances in conventional and nuclear weapons effectively eliminated any potential niche for their biological counterparts in kinetic models of

combat. Finally, the combination of munitions design, tactics, and agent selection would make military use of BW both conspicuous and attributable. The BWC and the general social aversion to the overt use of BW made the risk-reward balance associated with their employment unfavorable for state actors. Together, these conditions lead to an end of the first generation of kinetic BW programs[1, 2, 4-6, 43, 48, 49, 113].

As discussed earlier, conventional and nuclear weapons maintain their dominance as tools of kinetic warfare, and there remains no unique role for traditional biological weapons in the present day. However, as presented in Sections 1-2, the growing use of covert, gray zone warfare tactics has opened a novel niche that could be filled by a new type of biological weapon. Section 3 described how the COVID-19 pandemic provided a real-world case study that demonstrated alignment of the consequences of a global pandemic with many of the key objectives of gray zone warfare. This suggested the potential value of the covert use of weaponized pandemic pathogens in this context. Simultaneously, the same discussion also shed light on the ideal features of this new type of "pandemic biological weapon." Specifically, a viral agent capable of person-to-person transmission, with a high R_0 and with few effective medical countermeasures, could be particularly appropriate for this role.

Producing and deploying such an agent while maintaining plausible deniability remains non-trivial, but several enabling conditions have recently emerged that make this task more tractable now than ever before. This section will highlight several of those key enablers and will discuss how each could help facilitate gray zone biological warfare in the modern era.

Expanding Biomedical Knowledge. The first enabling factor is the rapid acceleration of general scientific knowledge. Analysis of scientific publications suggest that the growth rate of scientific knowledge is approximately exponential[114-117]. The rate has been estimated at approximately 4-5% per year, which suggests a knowledge doubling time of approximately 14-17 years[114]. Although the precise estimates of knowledge growth rates vary slightly according to the databases used for analysis, the regression models applied, and the knowledge subdomains under study, most estimates are comparable in magnitude[114-117].

The growth rate of the life sciences subdomain has been approximated at 5% per year, with a doubling time of just over 17 years[117]. The global biotechnology market continues to grow at an even

higher rate of approximately 11.8%[118], suggesting that enabling technologies will progressively become more readily available in this domain. Perhaps most relevant to the present discussion is knowledge growth in the field of virology. Analysis of a query of the Clarivate Web of Science publication database[119] for the terms ["virus" or " virology"] from the years 1940-2023 suggests exponential growth with an annual rate of 3% and an approximate doubling time of 23 years (Figure 1). This estimate is generally consistent with the overall life science trends[117], although it may err on the conservative side. Even so, this subset analysis suggests that knowledge of virology has doubled at least three times since the height of the first generation of BW in the 1960s. While a rapidly-growing knowledge base does not translate *de facto* into successful R&D efforts, it dose imply that the baseline of available information against which viral BW development activities would take place today is considerably more substantial than at any time in the past. The accelerating rate of knowledge growth, in general, and in the life sciences and virology, in particular, is the most general of all of the enablers that will be discussed herein, and it serves as the backdrop against which much of the subsequent discussion takes place.

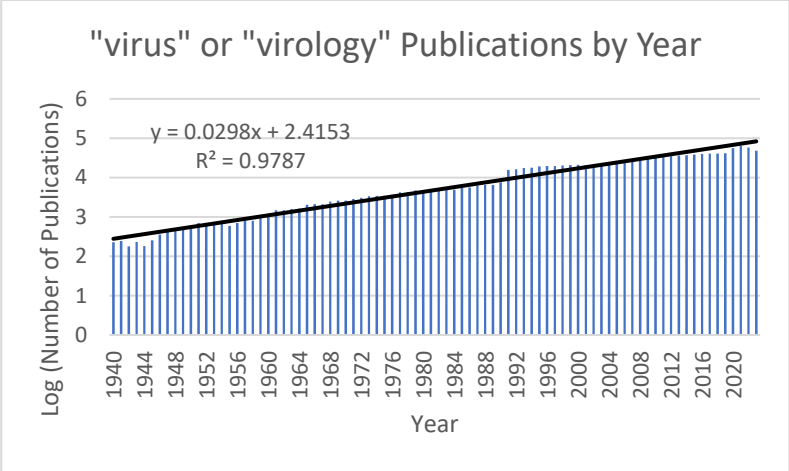

Figure 1 – Source Data from Clarivate Web of Science [119]

Emerging Biotechnologies. The life sciences knowledge base[117] and its derivative biotechnology sector continue to grow rapidly[118]. Within this space, several, specific emerging technologies have particular relevance to facilitating the design and bioengineering of potential viral BW. First, the emergence of whole-genome sequencing, followed over the past decade by progressive increases in the accuracy, speed, ease of use, and accessibility of these "next-generation sequencing" technologies[120], has provided critical insight into the basic genomic structure of pathogens. This, in turn, provides a roadmap for their manipulation by genetic engineering. To these ends, genome editing technologies have also made dramatic strides over the past decade[121, 122]. Perhaps the best-known among these technologies is the CRISPR-Cas9 method[123, 124], although numerous, other techniques have also become similarly commoditized and widely available[121, 122]. These technologies can be readily applied to molecular

engineering efforts with viral pathogens[125], potentially opening the door to a new era of viral BW R&D[126].

The potential health security implications of these technologies are readily apparent[126] and have sparked considerable debate[127-130]. Possibly the most prominent example of such controversy[131] surrounded the 2012 publications by Kawaoka et al.[132] and Fouchier et al.[133] regarding genetic modifications of the H5N1 influenza virus that increased its transmissibility. This began a heated scientific debate over the risks and benefits of gain-of-function (GoF) research[134]. Similarly, work by Cello et al.[135] describing *in vitro* synthesis of infectious poliovirus and by Evans et al.[136] detailing the *de novo* synthesis of the horsepox virus from commercially-synthesized DNA oligonucleotides amplified concerns regarding the biosecurity risks posed by modern synthetic biology[134, 137-140]. Most importantly for potential viral BW bioengineers, however, was the demonstration by these publications that, "no viral pathogen is likely beyond the reach of synthetic biology.[141]" Over the past several years, multiple, additional studies demonstrating similar viral molecular engineering work have been published and received with some controversy, and a complete account of all of this work is beyond the scope of this discussion. Although research innovation does not automatically translate into novel application, and while the debate continues regarding the balance between scientific discovery and biosecurity in the dual-use domains of GoF and synthetic biology research[142-144], there can be little debate about the potential value of these evolving methods for viral bioweapon engineering by states exploring the covert use of BW in gray zone warfare.

Proliferation of High-Containment Laboratories. Synthetic biology and GoF tools provide the methods for synthesis or modification of potential viral bioweapons, but the actual work on such organisms must be conducted in laboratory facilities designed from the ground-up with specialized capabilities and extensive safety measures. Such facilities are designated as Biosafety Level 4 (BSL-4)[145], and their sizeable footprint, their use of highly-specialized equipment and instrumentation, the considerable cost of their construction, and the heavy logistical burden associated with their operation make these facilities difficult to conceal. At the height of the first generation of state-sponsored BW programs, a relatively limited number of such facilities existed worldwide[146]. Chief among them were the US Army Biological Warfare Laboratories (USBWL) at Camp Detrick, Maryland[53], and the Soviet State Research Center of Virology and Biotechnology (VECTOR) in Koltsovo, Novosibirsk[5]. There was little doubt regarding the type of work being done at these institutes, and nearly all weaponized pathogens could trace their origins to one of

these two facilities. The scarcity of these labs effectively eliminated plausible deniability and simplified attribution associated with BW use, and thus covert use of BW was nearly impossible in that era.

Increasing demands for high-containment laboratories by governments, academia, and industry, however, has led to a marked proliferation of BSL-4 facilities worldwide[9]. The Global BioLabs Project, which tracks the proliferation of high-containment laboratories, has identified a total of 69 BSL-4s in operation or under construction as of 2023[146]. They are distributed across the globe, including 26 laboratories in Europe, 20 in Asia, and 15 in North America[146]. Similarly, there are 126 BSL-3+ facilities worldwide, which have only slightly less rigorous standards than BSL-4 laboratories and can also be used for engineering potential viral bioweapons[146]. Accordingly, it is not only the knowledge, laboratory methods, and technologies capable of facilitating pathogen bioengineering that are proliferating, but also the facilities in which such work can be performed.

The proliferation of high-containment laboratories is an enabler for covert BW development in two ways. First and most obviously, more facilities mean more availability of the physical resources necessary to conduct this type of work. However, a second benefit may be less obvious but even more valuable. The worldwide distribution of these facilities and their operation by governments, universities, and private industries creates a network across which covert BW R&D tasks can be carefully and deliberately distributed. Such an approach is similar in concept to *layering* activities in money laundering[147], wherein illicit funds are separated into smaller batches, spread across a series of various types of financial institutions, mixed with legitimate funds, and moved repeatedly until their origin is successfully obfuscated and attribution attempts are confounded. Layering of BW R&D preserves plausible deniability, which is paramount to the use of these agents for gray zone warfare, and the global proliferation of high-containment laboratories can be exploited to facilitate such an approach.

Advances in Computation and Artificial Intelligence. Knowledge, tools, and facilities are necessary but not sufficient for gray zone combatants to engineer novel viral pandemic bioweapons. The ability to apply that knowledge and to use those tools in novel ways to engineer a new biological weapon that exhibits a desired phenotype is also required. Human creativity and ingenuity will always be important drivers of such work, but the ability of scientists to conceive, initiate, and direct appropriate lines of R&D work has, historically, also been a key rate-limiting step in BW engineering. Advances in the speed and capability of computational resources, however, represent an enabling feature capable of accelerating this process. This is particularly true for artificial intelligence (AI) technologies[148], which hold promise for not only process optimization, but also for novel hypothesis generation. The details of the exponential growth of

computational power enjoyed in recent years, and the mechanisms by which it enables computationally-demanding processes, such as modeling, simulation, and AI, are beyond the scope of this discussion and are detailed elsewhere[149]. Here the focus will be placed on specific applications of these technologies that have the potential to facilitate or accelerate novel BW development or gray zone use of such agents.

AI technologies could be leveraged at several points in the R&D process of next-generation BW agents. The first such application is using AI to facilitate novel agent discovery and synthesis. Recent work by Urbina and colleagues[150, 151], for instance, illustrates the potential to leverage AI tools for discovery of novel chemical weapons (CW) agents. Using publicly-available data in conjunction with a published AI drug discovery tool[152], a standard desktop computer took less than six hours to return a list of 40,000 potential CW agents. This included the known nerve agent, VX, as well as multiple, novel compounds with greater predicted toxicity[150]. This simple exercise demonstrates the feasibility of using AI tools to accelerate hypothesis generation and discovery of lethal, laboratory-engineered agents. Proceeding a step further, these methods could then be used in conjunction with additional, AI-based tools to facilitate compound synthesis and production. The DeepSA model, for instance, predicts the synthesis accessibility of compounds in order to gauge their production capacity, and it has been tested against novel molecules suggested by various natural language processing discovery algorithms[153]. From here, tools such as ChemCrow, "a [large language model] chemistry agent designed to accomplish tasks across organic synthesis, drug discovery, and materials design[154]" could be used to autonomously plan and execute the synthesis of chemical compounds.

These aforementioned applications have thus far been confined to chemical design and synthesis, but extensions of these technologies to pathogen engineering is a logical next step. Accordingly, a second, related application involves leveraging AI biodesign tools for pathogen bioengineering[155]. The Nuclear Threat Initiative notes that, "AI biodesign tools provide insight into biological systems that would be very difficult for humans to generate on their own, and many experts believe that they could be misused by someone aiming to design toxins, pathogens, or other biological agents to cause harm.[155]" For example, Google DeepMind's AlphaFold[156] is an AI tool capable of predicting a protein's 3D folding pattern (tertiary structure) based on its amino acid sequence (primary structure). This holds significant potential for predicting protein functions and for engineering novel proteins; however, the United Nations Interregional Crime and Justice Research Institute (UNICRI) has also highlighted the dual-use potential of this technology by, "malicious actors," to weaponize protein-folding prediction[157]. Indeed, accurate and reliable computational prediction of protein folding, as well as similar AI biodesign tools, could be a significant asset in the hands of a BW molecular engineer.

Third, the potential for AI tools to predict pathogen traits, including transmissibility, host range, and virulence, from genome sequence data is currently being explored. "Experts in biological weapons pointed out that much of the challenge in developing an effective weapon is anticipating how it will interact with the complex world it is released into.[155]" This is a nascent field, but several recent studies have demonstrated the feasibility of these efforts. For example, the EVEscape tool, "combines fitness predictions from a deep learning model of historical sequences with biophysical and structural information," to, "quantif[y] the viral escape potential of mutations at scale and has the advantage of being applicable before surveillance sequencing, experimental scans or three-dimensional structures of antibody complexes are available.[158]" Similarly, the PHEVIR algorithm has been shown to predict accurately a variety of human disease states corresponding to the activities of several hundred viral and bacterial pathogens[159]. These are just two examples of AI tools that are working toward the goal of predicting the final, clinical disease characteristics from laboratory-level data. Such tools would be significant accelerators of pathogen bioengineering processes.

A fourth potential application of AI moves beyond the molecular level and into the implementation space. Large language models, a form of generative AI, may be used to suggest comprehensive strategies for facilitating the outbreak of a pandemic. A recent investigation of this approach found that, "In one hour...chatbots suggested four potential pandemic pathogens, explained how they can be generated from synthetic DNA using reverse genetics, supplied the names of DNA synthesis companies unlikely to screen orders, identified detailed protocols and how to troubleshoot them, and recommended that anyone lacking the skills to perform reverse genetics engage a core facility or contract research organization.[160]" Although a recent RAND Corporation report offered contradictory arguments suggesting that LLM technologies may not yet be robust enough for generating reliable plans for biological warfare[161], testimony regarding such scenarios before the US Senate Judiciary Committee emphasized that the emerging potential for national security risks associated with these approaches is demonstrable[162, 163]. Regardless of the absolute accuracy of present implementations of these high-level AI tools, the proof-of-principle work shows that AI applications in this space extend beyond agent design and into the realms of clinical prediction and logistical coordination in BW attacks.

Finally, at the highest level, AI and machine learning tools are being used to forecast epidemic dynamics. Modern dynamic pandemic forecasting involves using computational models and simulations to predict the spatiotemporal spread of diseases through a population[164, 165]. The current state-of-the-art employs deep learning systems[166] (e.g. long short-term memory models[167, 168]),

transformer-based models[169], and hybrid and ensemble methods[164, 170] to predict epidemic dynamics. Additionally, these models could be leveraged to predict the potential effects of various interventions on epidemic spread[171]. While mathematical models and simulations are only approximations of reality, the ability to predict the potential timeline and geographic spread of a disease and to anticipate the potential effects of selected control strategies would be valuable tools in planning gray zone BW attacks.

Evolving Sociopolitical Trends. Three evolving sociopolitical trends play an important role in creating an environment where gray zone use of a viral pandemic bioweapon may be seen as viable by a potential aggressor. This assessment is not designed to place a value judgement on any of these trends, as each has its own pros and cons that have been debated at length elsewhere. Rather, the purpose of this discussion is to note that the circumstances created by these trends can be exploited by a state actor to obscure their activities around the development and covert use of a viral pandemic bioweapon.

The first trend that could be exploited by a potential gray zone BW aggressor is *the normalization of R&D work involving gain-of-function (GoF) research.* The initial publication of the two, previously-mentioned papers[132, 133] regarding genetic modifications of the H5N1 influenza virus that increased viral transmissibility sparked considerable debate[172, 173] regarding the legal[174], ethical[175], public health[176], and biosecurity[177, 178] implications of this type of work. This initially led to restrictions on US federal funding for GoF work[179]. These were later rescinded[180] and replaced with explicit guidelines for funding such projects[181]. It is important to note, however, that the conduct of GoF research has never been restricted, only the policies regarding US governmental funding of such activities. A recent study by the Center for Security and Emerging Technology indicates that GoF research is prevalent and is conducted worldwide, with approximately 7,000 publications between 2000-2022 reporting GoF-type work conducted in at least 11 countries[182]. Of note, the study reports that approximately 47% of this work is conducted outside of the US and 33% is conducted within the confines of single institutions (without external collaboration or oversight). Additionally, 64% of the investigations involve research with viral pathogens, and 76% of that research is not related to vaccine development[182]. These figures suggest that a considerable amount of current viral GoF research may take place outside of the reach of rigorous oversight. The study further concludes that global GoF research will be difficult to regulate because of its prevalence, its potential valuable applications, and the, “varied and sometimes interconnected nature of [its] research ecosystem.[182]”

This data[182] is not included here in an attempt to imply that any type of illicit GoF work is currently taking place (BW-related or otherwise), but rather to illustrate the prevalence of this work, its disproportionate emphasis on viral pathogens, its worldwide distribution, and its inconsistent oversight. This is relevant to the present discussion, because a global research environment where GoF work is widespread, conducted in the open, and difficult to regulate can be exploited to provide viable cover for BW-related R&D work. When combined with layering strategies (see above) or couched in narratives supporting the peaceful applications of specific investigations, it could be possible for a motivated aggressor state to conduct a considerable amount of its BW R&D overtly. This differs from the nature of R&D work required to develop the first generation of bioweapons, where secrecy was paramount, covertness was commonplace, and efforts were geographically concentrated. Avoiding the need for secrecy and covert development work reduces R&D costs, accelerates the development timeline, and affords the opportunity to enlist human talent that might otherwise avoid explicit BW work[49].

Much of the work of a modern, state-sponsored R&D program for a viral pandemic pathogen weapon could be conducted in the open, under the guise of a vaccine or other research program. This would also allow the state to secure the assistance of a cadre of domestic (and even international collaborative) researchers who were ultimately unaware of the intended purpose of their work. Moreover, if any adverse biosafety event transpired (e.g. a "lab leak"), or if any covert BW work were to be uncovered, a cover story of altruistic GoF research could provide plausible deniability. In this way, the technological advances and prevalence of GoF research, combined with public opinion that is at least willing to tolerate the ongoing conduct of this work, create an opportunity wherein considerable R&D for a next-generation BW program can be conducted without the encumbrances associated with a need for secrecy and covertness.

The second trend that could be used to the advantage of a state developing a plan for next-generation biowarfare is *the current international public health collaboration environment.* In the wake of the COVID-19 pandemic, increased priority has been assigned globally to strengthening public health resources[183-186]. This commitment is reflected, for instance, in the United Nations Sustainable Development Goals (Goal 3, "Ensure healthy lives and promote well-being for all at all ages"[187]), the World Health Organization's Core Priorities ("Protecting against health emergencies"[188]), and the international embrace of the One Health Initiative[189]. The altruistic work of these initiatives and the growing spirit of international collaboration surrounding public health, however, can also be exploited to facilitate state-sponsored plans for gray zone BW use in several ways. First, the widely-recognized importance of domestic pandemic preparedness creates an environment where the hardening of internal

defenses against pandemics and pathogens raises no suspicions of ulterior motives. This can be exploited by an aggressor to strengthen domestic resilience infrastructure. Second, the open and public discourse regarding pandemic preparedness – including frank discussions by various nations regarding their own strengths and weaknesses to these ends – can provide valuable open-source intelligence on the state of preparedness of adversaries. This could be augmented by surreptitious, international collaborative initiatives on the part of the aggressor, the actual intent of which is to gain ground-level intelligence on the state of an opponent's technologies, preparedness, and response strategies. Finally, the growing emphasis on R&D in the pandemic preparedness space can be leveraged to provide additional cover and plausible deniability for BW development activities.

The third trend that could be leveraged to the advantage of a malevolent actor is *the growing recognition of the potential impacts of climate change on pandemic risk.* Much has been written in both the scientific literature[190-193] and in the lay press[194-197] regarding the potential for climate change to increase the risks of future pandemics, primarily by facilitating zoonotic spillover events [198-200]. Through deliberate selection of a zoonotic pathogen for weaponization and an appropriate geography for its initial release, a gray zone BW aggressor could leverage evolving awareness of the link between climate change and pandemic risk to create plausible deniability in the form of a spillover narrative. Taken together, scientific research regarding the risks of climate change as a pandemic catalyst and growing public awareness of this risk provide both a potential roadmap and a reasonable cover story for a gray zone BW attack.

SECTION 5: A GRAY-ZONE DEPLOYMENT SCENARIO FOR A VIRAL PANDEMIC BIOWEAPON

The discussion thus far has been theoretical, describing an emerging niche for viral pandemic bioweapons in gray zone warfare, illustrating how the COVID-19 pandemic could be interpreted by an aggressor as a real-world, proof-of-concept of the power of a global pandemic as a social and economic disruptor, and examining the unique set of evolving technologies and social trends that serve as enablers for the development and use of a next-generation BW. This section will now focus on the practical aspects of designing and executing a gray zone BW attack that is intended to cause social, political, and economic destabilization.

Strategic Objective. In the scenario outlined below, the overarching strategy involves a period of pre-attack, asymmetric preparation by the aggressor that will ultimately facilitate disproportionate resilience

to, and recovery from, the direct effects of a deliberate pandemic. Pathogen engineering and strategic deployment of the next-generation BW agent by the aggressor will be designed to maximize asymmetric damage to the under-prepared enemy populations and to the fabric of their societies. Simultaneously, the pandemic will create a period of atypical susceptibility of the enemy to deliberate information warfare and social engineering activities by the aggressor. These activities will be designed to influence both the public health response and the prevailing discourse about the crisis in such a way that the ultimate social experience and economic recovery are steered in directions that are disproportionately favorable to the attacker's interests. The net result will be post-pandemic global socioeconomic conditions that are more favorable for the attacker than those prevailing before the attack, which is the ultimate objective of gray zone warfare. The roadmap for this attack is divided into four phases: planning, preparation, execution, and modulation.

Planning. This phase involves careful analysis of the gaps that exists between current global socioeconomic conditions and those of a desired end state that is more favorable to the attacker. Once these gaps are identified and quantified, two categories of effects associated with a gray zone BW attack can be modeled and optimized to facilitate bridging the gaps. The first category involves analyzing both the direct and indirect effects that the pandemic itself will have on enemy societies. This includes human morbidity and mortality, the monetary and opportunity costs associated with the necessary public health response, and the effects on infrastructure, resource allocation, and economics in the targeted countries. These analyses will inform optimal parameter selection for engineering the bioweapon and for its deployment scenario. To these ends, modern computational power can be leveraged to conduct simulations of morbidity, mortality, economic costs, social effects, and economic consequences of pathogens associated with various R_0 values, lethality, long- versus short-term health effects, and treatment requirements. The COVID-19 experience can serve as a positive control, and data from that pandemic can help to calibrate these simulations. The second effects category that can be modeled and simulated comprises analyses designed to inform strategy and parameter selection for the information warfare and social engineering activities that will be conducted by the aggressor during the pandemic period. The details of this domain of the attack are beyond the scope of this paper; however, this is a critical aspect of shaping the post-pandemic world to the desired socioeconomic end state. Also of note, a valuable byproduct of these two categories of analysis will be insight into the nature and extent of domestic resilience required to maximize asymmetry in attack effects between the aggressor and the target societies.

The ultimate result of the planning phase will be threefold. First, the specific characteristics of a viral bioweapon that is optimally-suited to creating a pandemic optimized to serve the strategic objectives of the aggressor will be identified. These parameters will subsequently be used in the weapon R&D process. Second, a roadmap for the information warfare and social engineering aspects of the attack will be generated and can be used to plan those operations. Finally, required parameters for the nature and extent of domestic preparedness necessary for the aggressor to emerge from the pandemic in a disproportionately favorable state will be established. These will be used to guide subsequent preparation activities. Once all of these parameters have been established, the preparation phase can begin.

Preparation. This phase involves pre-attack work along four trajectories: weapon design, domestic preparedness, intelligence gathering, and information warfare planning. The previously-discussed global emphasis on pandemic preparedness means that at least the first three of these four lines of work can largely be conducted openly and without a need for either strict secrecy or covert action. Discussion of the fourth work stream, the information warfare strategy, is outside of the scope of this analysis and will not be discussed further but merits attention elsewhere.

The majority of work along the first trajectory, bioweapon design, can be conducted openly and publicly under the guise of anti-pandemic biomedical research. The current, permissive attitude towards GoF and gene editing research, combined with the global proliferation of high-containment laboratories, can be exploited to these ends. This work can also include R&D work on specific medical countermeasures against the intended bioweapon, which will be a valuable asset that can be leveraged strategically by the aggressor during the coming pandemic. A layering strategy, as outlined above, can be used to obfuscate the interconnectedness of these efforts, and only a small integration layer is required to be maintained behind the veil of state secrecy as the final common pathway. This structure also has the benefits of presenting the appearance of active participation in global anti-pandemic collaboration and of maintaining plausible deniability after the onset of the pandemic.

The majority of efforts along the second and third work streams, domestic preparedness and intelligence gathering, can also readily be conducted in the open. In the current, collaborative global environment of pandemic preparedness, states are expected to devote considerable resources to improving their domestic pandemic preparedness posture. Accordingly, even large-scale efforts in countermeasures stockpiling, public health infrastructure development, or resilience and preparedness exercises run little risk of raising any red flags in the global community. This starkly contrasts the sociopolitical climate of the 1980s, for instance, where a state's massing of biodefense resources would

likely be met with suspicion and concern by the rest of the world. Similarly, the current climate of information sharing in service of global pandemic preparedness provides an excellent opportunity for open-source intelligence gathering by the aggressor state regarding the biodefense capabilities of its opponents. In fact, the aggressor state may even be able to exploit the collaborative environment to avail itself of the technological innovations or excess resources that are freely offered by opposing states. As with the BW R&D, only a small subset of both domestic preparedness and foreign intelligence gathering activities need to be conducted by the aggressor covertly.

At the end of the preparation phase, the aggressor will possess a viral pandemic bioweapon that has been purpose-built to catalyze a global pandemic with precise features poised for strategic exploitation by the attacker. The precise nature of the weapon, including its virulence, its clinical phenotype, and the ideal method for its covert release, will have been dictated by and engineered according to the strategic objectives and operational plans of the aggressor. Simultaneously, the attacker will have developed a preparedness infrastructure that is tailor-made to maximize domestic resilience to the coming pandemic. This purpose-built infrastructure will minimize the domestic consequences of the pandemic and confer disproportionate, downstream advantage over opponents who have distributed their pandemic preparedness resources more broadly. The aggressor will also have gained extensive intelligence regarding the preparedness status of opponents, much of which has been offered freely in the spirit of global public health collaboration. Additionally, this entire system has also been engineered from the outset with an eye toward maintaining plausible deniability and avoiding attribution during the coming pandemic. At this point the stage is set for deployment of the weapon.

Execution. There are multiple possible scenarios for deploying the viral pandemic bioweapon, of which two will be considered here. With either approach, maximum priority is placed on plausible deniability and prevention of attribution. Moreover, because the intended consequences of the attack are global in scope, direct deployment within the geographic borders of the targeted state(s) is neither necessary nor advisable. These considerations shape the two deployment scenarios discussed below.

The first scenario involves release of the bioweapon in a geographic region that meets two criteria: (1) proximity to the primary intended target, and (2) an ecology that is known to present a risk for zoonotic spillover of viral diseases into human populations[201]. Examples include Central America, which has jungle ecologies and proximity to North and South America, North or Central Africa, which have a history of zoonotic spread and are in close proximity to Europe, and Central Asia[202], where emerging conditions are making novel zoonoses more probable. An ideal, specific site of pathogen release within such regions

would be a large population center that contains or is in close proximity to known risk environments for disease spill-over, including high-containment viral research laboratories, wild animal live meat markets ("wet markets"), extensive animal husbandry facilities, or nearby deforestation activities[203]. Additional, favorable conditions include active outmigration or irregular or mixed migrant flows from the region[204, 205] and sociopolitical circumstances that facilitate undetected disease spread or complicate international efforts for disease control near the source[206-208]. These additional parameters afford two distinct strategic advantages. First, release in a population center increases the probability of person-to-person spread, maximizes the number of transmission events, and presents ample opportunity for outmigration of infected patients from the region (e.g. air travel). Second, an ecology conducive to spillover and the presence of specific risk environments associated with such events increases plausible deniability for the aggressor.

The second scenario for release of the bioweapon involves carefully-controlled domestic release at an appropriately selected site within the attacker's own country. Superficially this seems counterintuitive because of the immediate creation of domestic casualties. However, the plausible deniability afforded by the inherently counterintuitive nature of this strategy is among its principal strategic advantages. To these ends, the COVID-19 experience in China is instructive. This approach also has several additional strategic advantages. First, it allows for maximal control of the inevitable, domestic effects of the pandemic from the outset. A release site can be chosen that maximizes the outflow of infected individuals to the enemy state, and it can be prospectively prepared for optimal domestic resilience. This includes optimizing local public health resources and preparing barriers to intra-state outmigration in advance, such that they can be implemented without delay after the initial outbreak. Second, a location that contains multiple risk environments for spillover events can be selected, which further increases plausible deniability of intentional release. Third, the initial appearance of the pandemic within the aggressor's own territory allows for controlled release of information by the state[209, 210]. This can be used as a stall tactic to allow the pandemic to take root before it is publicly disclosed. Fourth, access to early patients and clinical samples by international clinical coalitions can be controlled by the aggressor[211] in order to modulate intentionally the cadence of the global response. Finally, information related to a failed pathogen release attempt can be obscured from international view by domestic regulation of reporting, and subsequent, additional attempts to initiate the pandemic can be made domestically with impunity. The counter-argument that such a strategy is irrational for the aggressor will be addressed explicitly in Section 6. Once the pandemic has been initiated, the aggressor can begin the modulation phase.

Modulation. In this final phase, the aggressor has two objectives. First, it can influence the socioeconomic effects of the pandemic through coordinated information warfare operations. The details of this part of the modulation phase are outside the scope of this analysis. Second, it can influence the dynamics of the global response to the pandemic to align with strategic forecasts wherein its asymmetric post-pandemic advantages are maximized. This can be accomplished by leveraging its unique, pre-pandemic preparation strategies. For example, as mentioned above, it can delay early global pandemic mitigation strategies by controlling the release of information and by restricting access to domestic patients and clinical samples. Simultaneously, it can choose to make available to the world its preemptively stockpiled medical supplies and resources, in a manner and at a rate that best suits its operational plan. Similarly, if it has proactively created effective countermeasures, it can gain global prestige by appearing to "develop" these countermeasures at a pace that exceeds its global competitors, and it can kindle international favor and reputational benefits by making these countermeasures available globally at a time of its choosing. In this fashion, the aggressor can covertly influence the global tempo of the pandemic in a fashion that best accomplishes its gray zone objectives, and it can position itself to be viewed disproportionately favorable by citizens of its enemy and of the world at large.

Summary. This discussion is not meant to serve as an exhaustive roadmap for deliberate pandemic engineering, nor has every operational element been explored in detail. Rather, it is intended to bridge the gap between the theoretical and the practical domains of this novel scenario for gray zone use of next-generation BW by illustrating the art of the possible. In this way, it illustrates the opportunities and consequences afforded by the modern facilitators of covert BW operations (Section 4) in the context of the changing nature of warfare objectives and tactics (Sections 1-2) and in the post-COIVD era (Section 3). Ultimately, these discussions illustrate that current conditions may be more conducive to covert, next-generation, biological warfare than many may believe, and that gray zone warfare using pandemic biological weapons may not be as technically difficult as some may assume.

SECTION 6: SELECTED COUNTER-ARGUMENTS

The current analysis suggests that next-generation bioweapons in the form of viral pandemic pathogens may be a novel and viable strategy for gray zone warfare. However, several reasonable counter-arguments can be made against such a strategy. Four of these are discussed below.

Counterpoint 1: Fear of violating the BWC and associated international norms against BW use would deter an aggressor from taking this approach. Much has been written about the value of the 1975 BWC[6], particularly regarding its lack of enforcement provisions[212-214]. It is generally considered to be a relatively weak treaty in-and-of itself, and so it seems unlikely that being signatory to the treaty alone would provide sufficient deterrence to a motivated aggressor. The real power of the BWC, however, is the strongly held international norms against BW use that it reflects[51, 215]. Although some argue that these norms are not absolute[216] and are progressively eroding[107, 217, 218], biological warfare is still widely considered to be unacceptable in modern society[215]. A state that could be proven definitively to have perpetrated a large-scale BW attack risks immediate relegation to international pariah status. The leadership, military, and economy of such a state would suffer considerably for their role in these actions, and it could take decades of contrition and remediation before the aggressor state would be received back into the international community.

The deterrent value of this argument hinges on two issues. First, how motivated is the aggressor to gain and exploit a gray zone advantage to facilitate its rise to global prominence, and is the very real risk of alienation one that it is willing to take in service of its ambition? Second, how certain is the aggressor that they will be able to maintain plausible deniability after conducting such an attack? Addressing these issues would, undoubtedly, be a major part of a state's decision to pursue the covert use of pandemic biological weapons.

Counterpoint 2: Engineering a viral pandemic pathogen is not trivial and may not be achievable, even with modern scientific knowledge and biotechnology resources. Simply because the world knows more about viral biology than ever before and possesses technologies that facilitate pathogen genome engineering[126], it is not a foregone conclusion that even a motivated state would be able to successfully design or deliver an engineered pandemic biological weapon[49, 219]. Additionally, even if the technical challenges could be mastered, there are well-described organizational barriers that have historically complicated state-sponsored attempts to develop BW programs[49]. The previous discussion is not intended to minimize the technical and institutional challenges associated with producing such an agent, and considerable R&D efforts would be required on the part of the aggressor to realize this plan. Indeed, the Soviet viral BW program took many years to make modest progress in the 1980s[5], although they did not have the advantage of modern enabling technologies at their disposal. In the end, it may prove to be a race between competing R&D programs that determine the technological feasibility of the proposed

gray zone attack strategy. Specifically, the race to produce a viable pandemic biological weapon by the aggressor must outpace the acceleration in molecular forensic attribution capabilities[103, 105, 220, 221]. Once pathogen attribution becomes accurate and reliable, the utility of this attack strategy will evaporate and the discussion will become moot.

Counterpoint 3: This attack strategy necessarily involves a state causing its own domestic casualties, and this will be unacceptable to the state. This is a powerful argument in the context of a state that places primacy on the value of the lives of its citizens. Unfortunately, history has taught that this primacy is not universal among all political regimes[222, 223]. Therefore, the viability of this attack strategy in the eyes of the aggressor state will depend on the way that its regime weighs the strategic advantages it offers relative to the human costs that it is willing to incur. It can be argued that this type of decision has been made by ruling regimes for centuries, as every decision to attack an enemy is laden with the expectation that both military and civilian casualties will be sustained by the attacker. While some may emphasize that deliberately inflicting disease on one's own citizens is inherently different from expecting civilian deaths during a period of war, a counterargument regarding the fundamental similarities of the ultimate consequences of each scenario could also be made. Ultimately, this counterargument's power depends on the perspective of the regime that presides over the aggressor state, and potential target states would be wise to consider that those attitudes may differ relative to their own social norms.

Counterpoint 4: Even with careful planning, a pandemic inherently becomes less predictable as it evolves. The potential to lose control over the pandemic it creates represents an unacceptable risk to the attacker. The lack of predictability and control over BW has been a strong argument against their use for decades[224, 225], and it remains applicable to the present scenario. Two considerations are relevant to these ends. First, a fundamental difference between a pandemic biological weapon and a traditional BW is that self-propagation through human-to-human transmission is a deliberate feature of the former, whereas the latter tended to require direct exposure to weaponized pathogen. An aggressor considering this attack strategy would, necessarily, conduct careful risk modeling and simulation of downstream events in order to better understand the scope of the possible evolution of the pandemic that they are unleashing and would craft appropriate contingency scenarios. Like all simulations, there will be uncertainty associated with all of these models, but this is a feature of all war planning. The degree to which the aggressor is confident in their predictions and is, simultaneously, willing to accept the uncertainties associated with their models, will directly influence their decision to employ the strategy. Second, it can

be argued that a military can always stop a kinetic attack or withdraw troops if circumstances on the battlefield change, but it is considerably more difficult to stop a self-propagating pandemic once it has been unleashed. This is only true, however, if the attacker does not possess effective countermeasures against the pathogen. An attacker in possession of a viable treatment or cure could "retreat" in response to unanticipated conditions by releasing the countermeasure to the world. In the context of modern biotechnology, and during a pandemic, the attacker could attribute its possession of the countermeasure to the success of its domestic R&D sector, and it may even be hailed as a global hero for bringing about the end of the pandemic. Notwithstanding, the emergence of unanticipated mutations[226] could moderate this capability, so the probability of unexpected loss of control must still be modeled. Therefore, the validity of this argument hinges both on the confidence of the attacker in their pre-attack risk models and contingency plans and on the proprietary availability of effective medical countermeasures at the time of the attack.

CONCLUSIONS

This analysis has examined the potential viability of a grey zone attack strategy by a state aggressor using a next-generation biological weapon in the form of a viral pandemic pathogen (engineered or wild type) to catalyze a pandemic. Such an agent has been referred to herein as a "pandemic biological weapon." The details of the pandemic that such a weapon unleashes, including its clinical characteristics and the tempo of its evolution, can be tailored (at least broadly) to the strategic needs of the aggressor, and the attacker can use various information warfare and social engineering strategies during the pandemic period to influence public opinion and economic markets in a manner that is consistent with its gray zone objectives.

The changing nature of warfare, shifting from kinetic to more covert, creates a niche for such an attack. The global experience with the COVID-19 pandemic has illustrated the disruptive influence that pandemics can have on modern societies. This includes not only casualties and clinical consequences, but also social, political, and economic effects. Additionally, the recent pandemic illustrates the difficulty that target states may have in preventing the spread of a weaponized pandemic, and it also suggests that a combination of careful planning by the aggressor and current limitations in the nascent field of microbial forensics could help to preserve plausible deniability by complicating definitive attribution. While such an attack with a biological weapon was previously impractical due to the combination of a focus on kinetic BW delivery mechanisms and emphasis of bacterial pathogens, several features of modern society now

make such an attack more technically feasible than ever before. These include a general increase in biomedical knowledge, particularly in the domain of virology, and the rapidly accelerating growth of biotechnologies that have commoditized genome sequencing and gene editing. These technical advances coalesce with a social context in which high-containment laboratories are proliferating and gene editing and gain-of-function research are becoming commonplace to create an environment where considerable pathogen R&D could be conducted overtly by the aggressor state. A decreasing requirement for covert operations, combined with increasing global efforts to promote public health infrastructure development and international transparency in pandemic prevention, can be exploited by an aggressor both to accelerate the pace of its BW R&D and to gather open-source intelligence on the resiliency status of enemy states. Together, these factors merge to create the most conducive circumstances in modern history for the development of a pandemic biological weapon. Even more concerning, lessons learned from the COVID-19 pandemic suggest that there may be viable, practical strategies for the covert deployment of such an agent, and that application of modern information warfare and social engineering methods during the period of global turmoil introduced by an engineered pandemic could further service the strategic objectives of the gray zone aggressor.

This plan is not foolproof, and reasonable counterarguments can be made against such a covert attack model. These include the risks to the aggressor associated with violating international norms against BW use and the risks of being relegated to the status of a global pariah if the attacker were identified. This is contingent upon successful attribution, however, and this is far from reliable at present. Similarly, even if the science and biotechnology resources for engineering such a pathogen are sufficient, there are various technical and organizational challenges to successful development of such a weapon. These challenges, however, lessen by the day. Additionally, the attacker would have to be willing to tolerate domestic casualties and costs that may be considerable, and they risk deploying a weapon that is inherently unpredictable and over which they may not be able to retain sufficient control. Still, for an aggressor that is highly risk-tolerant, heavily-motivated to achieve global prominence at all costs, and willing to accept domestic casualties in service of its overarching ambitions, an attack using an engineered pandemic biological weapon presents a novel and potentially viable strategy for achieving asymmetric advantage in the modern arena of gray zone warfare.

REFERENCES

1. Riedel, S., *Biological warfare and bioterrorism: a historical review.* Proc (Bayl Univ Med Cent), 2004. **17**(4). p. 400-6.
2. Frischknecht, F., *The history of biological warfare. Human experimentation, modern nightmares and lone madmen in the twentieth century.* EMBO Rep, 2003. **4 Spec No**(Suppl 1). p. S47-52.
3. Keiichi, T., *Unit 731 and the Japanese Imperial Army's Biological Warfare Program.* The Asia-Pacific Journal, 2005. **3**(11).
4. Barenblatt, D., *A plague upon humanity : the secret genocide of Axis Japan's germ warfare operation*. 1st ed. 2004, New York: HarperCollins Publishers. Available from: http://www.loc.gov/catdir/description/hc042/2003051051.html.
5. Leitenberg, M., R.A. Zilinskas, and J.H. Kuhn, *The Soviet biological weapons program : a history*. 2012, Cambridge, Massachusetts: Harvard University Press.
6. *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weaopns and on their Destruction*. United Nations. 1972. Available from: https://front.un-arm.org/wp-content/uploads/2020/12/BWC-text-English-1.pdf.
7. Zubok, V.M., *Collapse: The Fall of the Soviet Union*. 2021: Yale University Press. Available from: http://www.jstor.org/stable/j.ctv1zvccnm.
8. National Academies of Sciences, E., et al., *Preparing for Future Products of Biotechnology*. 2017, Washington (DC): National Academies Press (US).
9. Peters, A., *The global proliferation of high-containment biological laboratories: understanding the phenomenon and its implications.* Rev Sci Tech, 2018. **37**(3). p. 857-883.
10. Gilsdorf, J.R. and R.A. Zilinskas, *New Considerations in Infectious Disease Outbreaks: The Threat of Genetically Modified Microbes.* Clinical Infectious Diseases, 2005. **40**(8). p. 1160-1165. Available from: https://doi.org/10.1086/428843.
11. de Oliveira, T. and H. Tegally, *Will climate change amplify epidemics and give rise to pandemics?* Science, 2023. **381**(6660). p. eadk4500.
12. Antràs, P., S.J. Redding, and E. Rossi-Hansberg, *Globalization and Pandemics.* American Economic Review, 2023. **113**(4). p. 939-81. Available from: https://www.aeaweb.org/articles?id=10.1257/aer.20201479.
13. *A National Blueprint for Biodefense. Report of the Bipartisan Commission on Biodefense*. Bipartisan Commission on Biodefense. 2015. Available from: https://biodefensecommission.org/wp-content/uploads/2015/10/National-Blueprint-for-Biodefense-2021_reprint_v4_web-1.pdf.
14. Klotz, L.C. and E.J. Sylvester, *Breeding Bio Insecurity: How U.S. Biodefense Is Exporting Fear, Globalizing Risk, and Making Us All Less Secure*. 2009, University of Chicago Press.
15. Smith, F.L., *American biodefense : how dangerous ideas about biological weapons shape national security*. Cornell studies in security affairs. 2014, Ithaca: Cornell University Press.
16. Zhou, D., et al., *Biosafety and biosecurity.* J Biosaf Biosecur, 2019. **1**(1). p. 15-18.
17. Keegan, J., *A history of warfare*. 1993, New York: Alfred A. Knopf : Distributed by Random House, Inc. Available from: http://www.loc.gov/catdir/description/random047/93014884.html.
18. Freedman, L. *Russia and the new language of war*. The New Statesman. 2023. Available from: https://www.newstatesman.com/world/europe/ukraine/2023/03/russia-new-language-war-cyber-attack.
19. Esposito, V.J., *War as a Continuation of Politics.* Military Affairs, 1954. **18**(1). p. 19-26. Available from: http://www.jstor.org.mutex.gmu.edu/stable/1982704.
20. Sunzi, R.D. Sawyer, and M.-c.n. Sawyer, *The art of war*. 1st ed. History and warfare. 1994, Boulder, Colo: Westview Press.

21. Clausewitz, C.v., et al., *On war*. 1984, Princeton, N.J: Princeton University Press.
22. Liang, Q. and W. Xiangsui, *The science of military strategy*. 1999, Beijing: National Defense University Press.
23. DOD. *Summary of the Irregular Warfare Annex to the National Defense Strategy*. United States Department of Defense. 2020. Available from: https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF.
24. Chester, K. *Rights and Wrongs: Adopting Legitimacy as the Tenth Principle of War*. School of Advanced Military Studies, United States Army Command and General Staff College. 2000. Available from: https://apps.dtic.mil/sti/tr/pdf/ADA391149.pdf.
25. Ucko, D. and T. Marks. *Redefining Irregular Warfare: Legitimacy, Coercion, and Power*. Modern War Institute at West Point. 2022. Available from: https://mwi.westpoint.edu/redefining-irregular-warfare-legitimacy-coercion-and-power/.
26. Artiaga, S. *Contrasting Chinese and American Approaches to Irregular Warfare*. Insights, US Department of Defense Irregular Warfare Center. 2024. Available from: https://irregularwarfarecenter.org/wp-content/uploads/I15_Contrasting-Chinese-and-American-Approaches-to-Irregular-Warfare.pdf.
27. Endo, T. *The Conceptual Definition of "Irregular Warfare" and the Today's International Security Environment*. Proceedings of teh 2017 International Forum on War History. Translated from Japanese by the Japanese National Institute for Defense Studies. 2023. Available from: https://www.nids.mod.go.jp/english/event/forum/pdf/2017/04_endo.pdf.
28. Larson, E.V., et al., *Assessing Irregular Warfare: A Framework for Intelligence Analysis*. 2008, Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/monographs/MG668.html.
29. CRS. *Defense Primer: What Is Irregular Warfare?* Congressional Research Service. 2024. Available from: https://crsreports.congress.gov/product/pdf/IF/IF12565.
30. Monaghan, S., *Countering Hybrid Warfare: So What for the Future Joint Force?* PRISM, 2019. **8**(2). p. 82-99. Available from: https://www.jstor.org/stable/26803232.
31. Gerasimov, V. *The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*. Military-Industrial Kurier. Translated in Military Review. 2013. Available from: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf.
32. Votel, J.L., et al., *Unconventional Warfare in the Gray Zone.* Joint Force Quarterly : JFQ, 2016. (80). p. 101-109. Available from: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf.
33. Azad, T.M., M.W. Haider, and M. Sadiq, *Understanding Gray Zone Warfare from Multiple Perspectives.* World Affairs, 2022. **186**(1). p. 81-104. Available from: https://journals.sagepub.com/doi/10.1177/00438200221141101.
34. Harrington, J. and R. McCabe. *Detect and Understand: Modernizing Intelligence for the Gray Zone*. Centerf or Strategic and International Studies. 2021. Available from: https://www.csis.org/analysis/detect-and-understand-modernizing-intelligence-gray-zone.
35. Mazarr, M.J. *Mastering the gray zone: understanding a changing era of conflict*. 2015. Available from: https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1427&context=monographs.
36. Schadlow, N. *Peace and War: The Space Between*. War on the Rocks. 2014. Available from: https://warontherocks.com/2014/08/peace-and-war-the-space-between/.

37. Lin, B., et al., *Competition in the Gray Zone: Countering China's Coercion Against U.S. Allies and Partners in the Indo-Pacific*. 2022, Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/research_reports/RRA594-1.html.
38. Troeder, E. *A Whole-of-Government Approach to Gray Zone Warfare*. US Army War College Press. 2019. Available from: https://press.armywarcollege.edu/monographs/937.
39. DNI. *The Future of the Battlefield*. United States National Intelligence Council Strategic Futures Group, Office of the Director of National Intelligence. 2021. Available from: https://www.dni.gov/files/images/globalTrends/GT2040/NIC-2021-02493--Future-of-the-Battlefield--Unsourced--14May21.pdf.
40. Jones, S., et al. *Competing Without Fighting: China's Strategy of Political Warfare*. Center for Strategic and International Studies. 2023. Available from: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-08/230802_Jones_CompetingwithoutFighting.pdf?VersionId=Zb5B2Le0lf0kk7.QH7E0meA9phGqQEZf.
41. Jonsson, O., *The Russian Understanding of War: Blurring the Lines between War and Peace*. 2019: Georgetown University Press. Available from: http://www.jstor.org/stable/j.ctvr697c8.
42. Arreguín-Toft, I., *How the Weak Win Wars: A Theory of Asymmetric Conflict.* International Security, 2001. **26**(1). p. 93-128. Available from: http://www.jstor.org.mutex.gmu.edu/stable/3092079.
43. DOD. *The Militarily Critical Technologies List. Part II: Weapons of Mass Destruction Technologies*. United States Department of Defense. 1998. Available from: https://irp.fas.org/threat/mctl98-2/mctl98-2.pdf.
44. Wheelis, M., L. Rózsa, and M. Dando, *Deadly cultures : biological weapons since 1945*. 2006, Cambridge, Mass.: Harvard University Press. Available from: http://www.loc.gov/catdir/toc/fy0613/2005050225.html.
45. *US Policy on Chemical And Biological Warfare Agents*. Interdepartmental Political-Military Group, United States Department of State. 1969. Available from: https://2001-2009.state.gov/documents/organization/90902.pdf.
46. Guillemin, J., *Scientists and the history of biological weapons. A brief historical overview of the development of biological weapons in the twentieth century.* EMBO Rep, 2006. **7 Spec No**(Spec No). p. S45-9.
47. Matthews, L., et al. *Plagues, Cyborgs, and Supersoldiers: The Human Domain of War*. RAND Corporation. 2023. Available from: https://www.rand.org/pubs/research_reports/RRA2520-1.html.
48. Croddy, E.A. and J.J. Wirtz, *Weapons of Mass Destruction [2 Volumes]: An Encyclopedia of Worldwide Policy, Technology, and History*. 2005: Bloomsbury Academic. Available from: https://books.google.com/books?id=ZzlNgS70OHAC.
49. Ben Ouagrham-Gormley, S., *Barriers to bioweapons : the challenges of expertise and organization for weapons development*. Cornell studies in security affairs. 2014, Ithaca: Cornell University Press.
50. Galamas, F., *Biological Weapons, Nuclear Weapons and Deterrence: The Biotechnology Revolution.* Comparative Strategy, 2008. **27**(4). p. 315-323. Available from: https://doi.org/10.1080/01495930802358364.
51. Bentley, M. *The Biological Weapons Taboo - War on the Rocks*. War on the Rocks. 2023. Available from: https://warontherocks.com/2023/10/the-biological-weapons-taboo.
52. Siman, B. *Hybrid Warfare: Attribution is Key to Deterrence*. Egmont Royal Institute for International Relations. 2023. Available from: https://www.egmontinstitute.be/hybrid-warfare-attribution-is-key-to-deterrence/.

53. Bozue, J., et al., *Medical aspects of biological warfare*. 2. ed. Textbooks of military medicine. 2018, Fort Sam Houston, Texas: Office of the Surgeon General, Borden Institute, US Army Medical Department Center and School, Health Readiness Center of Excellence.
54. Patterson, G.E., et al., *Societal Impacts of Pandemics: Comparing COVID-19 With History to Focus Our Response.* Front Public Health, 2021. **9**: p. 630449.
55. Sampath, S., et al., *Pandemics Throughout the History.* Cureus, 2021. **13**(9). p. e18136.
56. Polat, M., S. Burmaoglu, and O. Saritas, *COVID-19 and Society: Socio-Economic Perspectives on the Impact, Implications, and Challenges*. 2022: Springer International Publishing. Available from: https://link.springer.com/book/10.1007/978-3-031-13142-4.
57. Jørgensen, F., et al., *Pandemic fatigue fueled political discontent during the COVID-19 pandemic.* Proceedings of the National Academy of Sciences, 2022. **119**(48). p. e2201266119. Available from: https://doi.org/10.1073/pnas.2201266119.
58. Reid, J.C., S.J. Brown, and J. Dmello, *COVID-19, Diffuse Anxiety, and Public (Mis)Trust in Government: Empirical Insights and Implications for Crime and Justice.* Crim Justice Rev, 2023.
59. Hough, M., et al., *Procedural Justice, Trust, and Institutional Legitimacy.* Policing: A Journal of Policy and Practice, 2010. **4**(3). p. 203-210. Available from: https://doi.org/10.1093/police/paq027.
60. Šrol, J., V. Čavojová, and E. Ballová Mikušková, *Finding Someone to Blame: The Link Between COVID-19 Conspiracy Beliefs, Prejudice, Support for Violence, and Other Negative Social Outcomes.* Front Psychol, 2021. **12**: p. 726076.
61. Edelson, J., et al., *The effect of conspiratorial thinking and motivated reasoning on belief in election fraud.* Political Research Quarterly, 2017. **70**(4). p. 933-946.
62. Woods, E.T., et al., *COVID-19, nationalism, and the politics of crisis: A scholarly exchange.* Nations and Nationalism, 2020. **26**(4). p. 807-825. Available from: https://doi.org/10.1111/nana.12644.
63. Borkowska, M. and J. Laurence, *Coming together or coming apart? Changes in social cohesion during the Covid-19 pandemic in England.* European Societies, 2021. **23**(sup1). p. S618-S636. Available from: https://doi.org/10.1080/14616696.2020.1833067.
64. Buizza, C., et al., *Impact of COVID-19 Pandemic on Well-Being, Social Relationships and Academic Performance in a Sample of University Freshmen: A Propensity Score Match Evaluation Pre- and Post-Pandemic.* Int J Environ Res Public Health, 2023. **20**(15).
65. Khan, A.S., et al., *The impact of coronavirus crisis on human interpersonal relationships among AlAhsa population.* Ann Afr Med, 2024. **23**(1). p. 76-81.
66. Long, E., et al., *COVID-19 pandemic and its impact on social relationships and health.* J Epidemiol Community Health, 2022. **76**(2). p. 128-132.
67. Sundler, A.J., et al., *Adolescents' and young people's experiences of social relationships and health concerns during COVID-19.* Int J Qual Stud Health Well-being, 2023. **18**(1). p. 2251236.
68. Wollebæk, D., A. Fladmoe, and K. Steen-Johnsen, *'You can't be careful enough': Measuring interpersonal trust during a pandemic.* Journal of Trust Research, 2021. **11**(2). p. 75-93. Available from: https://doi.org/10.1080/21515581.2022.2066539.
69. Pinto, S. *The Pandemic's Effects on Children's Education*. Federal Reserve Bank of Richmond, Economic Brief No. 23-29. 2023. Available from: https://www.richmondfed.org/publications/research/economic_brief/2023/eb_23-29.
70. Kuhfeld, M., J. Soland, and K. Lewis. *Test Score Patterns Across Three COVID-19-impacted School Years*. Annenberg Institute, Brown University, Ed Working Paper 22-521. 2022. Available from: https://edworkingpapers.com/sites/default/files/ai22-521.pdf.
71. Kuhfeld, M., et al. *The pandemic has had devastating impacts on learning. What will it take to help students catch up?* Brookings Institution. 2022. Available from:

https://www.brookings.edu/articles/the-pandemic-has-had-devastating-impacts-on-learning-what-will-it-take-to-help-students-catch-up/.
72. Leiws, K. and M. Kuhfeld. *Education's long COVID: 2022–23 achievement data reveal stalled progress toward pandemic recovery*. Center for School and Student Progress. 2023. Available from: https://www.nwea.org/uploads/Educations-long-covid-2022-23-achievement-data-reveal-stalled-progress-toward-pandemic-recovery_NWEA_Research-brief.pdf.
73. Mazur, M., M. Dang, and M. Vega, *COVID-19 and the march 2020 stock market crash. Evidence from S&P1500.* Finance Research Letters, 2021. **38**: p. 101690. Available from: https://www.sciencedirect.com/science/article/pii/S1544612320306668.
74. IMF. *World Economic Outlook, April 2020: The Great Lockdown*. International Monetary Fund. 2020. Available from: https://www.imf.org/-/media/Files/Publications/WEO/2020/April/English/text.ashx.
75. OECD. *International trade during the COVID-19 pandemic: Big shifts and uncertainty*. Organisation for Economic Co-operation and Development. 2022. Available from: https://read.oecd-ilibrary.org/view/?ref=1129_1129345-casormobh7&title=International-trade-during-the-COVID-19-pandemic.
76. Siegel, R., A. VanDam, and E. Werner. *2020 was the worst year for economic growth since World War II*. The Washington Post. 2021. Available from: https://www.washingtonpost.com/business/2021/01/28/gdp-2020-economy-recession/.
77. *GDP Growth (annual 5) - Euro Area*. World Bank Open Data. Available from: https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?locations=XC.
78. *Industries Most and Least Impacted by COVID-19 from a Probability of Default Perspective - January 2022 Update*. S&P Global Market Intelligence. 2022. Available from: https://www.spglobal.com/marketintelligence/en/news-insights/blog/industries-most-and-least-impacted-by-covid-19-from-a-probability-of-default-perspective-january-2022-update.
79. Decker, R. and J. Haltiwanger. *Business entry and exit in the COVID-19 pandemic: A preliminary look at official data*. Board of Governors of the Federal Reserve System. 2022. Available from: https://www.federalreserve.gov/econres/notes/feds-notes/business-entry-and-exit-in-the-covid-19-pandemic-a-preliminary-look-at-official-data-20220506.html.
80. *Unemployment rate rises to record high 14.7 percent in April 2020*. US Bureau of Labor Statistics. 2020. Available from: https://www.bls.gov/opub/ted/2020/unemployment-rate-rises-to-record-high-14-point-7-percent-in-april-2020.htm.
81. *Unemployment, total (% of total labor force) (modeled ILO estimate)*. World Bank Open Data. 2024. Available from: https://data.worldbank.org/indicator/SL.UEM.TOTL.ZS.
82. *American Rescue Plan Two Years In: The American Rescue Plan Act's Historic Investments In A Stronger Economic Future*. United States Department of Treasury. 2023. Available from: https://home.treasury.gov/system/files/136/Two-Year-ARP-Anniversary-Report.pdf.
83. Konczal, M. *Inflation in 2023: Causes, Progress, and Solutions.. Testimony before the House Committee on Oversight and Accountability Subcommittee on Health Care and Financial Services*. Roosavelt Institute. 2023. Available from: https://oversight.house.gov/wp-content/uploads/2023/03/inflation_testimony_mkonczal_current.pdf.
84. *World Economic Outlook 2023 - A Rocky Reocvery*. International Monetary Fund. 2023. Available from: https://www.imf.org/en/Publications/WEO/Issues/2023/04/11/world-economic-outlook-april-2023.
85. CRS. *Global Economic Effects of COVID-19*. Congressional Research Service. 2021. Available from: https://crsreports.congress.gov/product/pdf/R/R46270/82.

86. McKibbin, W. and R. Fernando, *The global economic impacts of the COVID-19 pandemic.* Economic Modelling, 2023. **129**: p. 106551. Available from: https://www.sciencedirect.com/science/article/pii/S0264999323003632.
87. Spence, A. *Economic decline is leading to political instability. What's the solution?* World Economic Forum. 2016. Available from: https://www.weforum.org/agenda/2016/03/economic-decline-is-leading-to-political-instability-whats-the-solution/.
88. Wilcox, J. *Economic Instability Endangers Democracy*. Center for the National Interest. 2017. Available from: https://nationalinterest.org/feature/economic-instability-endangers-democracy-23560?nopaging=1.
89. Aisen, A. and F. Veiga. *How Does Political Instability Affect Economic Growth*. International Monetary Fund. 2010. Available from: https://www.imf.org/external/pubs/ft/wp/2011/wp1112.pdf.
90. Hadzi-Vaskov, M., S. Pienknagura, and L. Ricci. *The Macroeconomic Impact of Social Unrest*. International Monetary Fund. 2021. Available from: https://www.imf.org/en/Publications/WP/Issues/2021/05/07/The-Macroeconomic-Impact-of-Social-Unrest-50338.
91. *A History of the Public Health System*, in *The Future of Public Health*. 2000, Committee for the Study of the Future of Public Health, Division of Health Care Services, National Academy of Sciences.Available from: https://www.ncbi.nlm.nih.gov/books/NBK218224/.
92. Bok, K., et al., *Accelerated COVID-19 vaccine development: milestones, lessons, and prospects.* Immunity, 2021. **54**(8). p. 1636-1651.
93. Annabel, F., *BMJ readers choose the "sanitary revolution" as greatest medical advance since 1840.* BMJ, 2007. **334**(7585). p. 111. Available from: http://www.bmj.com/content/334/7585/111.2.abstract.
94. Agyapon-Ntra, K. and P.E. McSharry, *A global analysis of the effectiveness of policy responses to COVID-19.* Scientific Reports, 2023. **13**(1). p. 5629. Available from: https://doi.org/10.1038/s41598-023-31709-2.
95. Haug, N., et al., *Ranking the effectiveness of worldwide COVID-19 government interventions.* Nature Human Behaviour, 2020. **4**(12). p. 1303-1312. Available from: https://doi.org/10.1038/s41562-020-01009-0.
96. Ioannidis, J.P.A., *The end of the COVID-19 pandemic.* Eur J Clin Invest, 2022. **52**(6). p. e13782.
97. Antia, R. and M.E. Halloran, *Transition to endemicity: Understanding COVID-19.* Immunity, 2021. **54**(10). p. 2172-2176.
98. CDC. *COVID Data Tracker*. Centers for Disease Control and Prevention. 2024. Available from: https://covid.cdc.gov/covid-data-tracker/#datatracker-home.
99. Graham, M.H. and S. Singh, *An Outbreak of Selective Attribution: Partisanship and Blame in the COVID-19 Pandemic.* American Political Science Review, 2024. **118**(1). p. 423-441. Available from: https://www.cambridge.org/core/product/C869E5F854BE66E1822F6E34E3116E94.
100. Gostin, L.O. and G.K. Gronvall, *The Origins of Covid-19 — Why It Matters (and Why It Doesn't).* New England Journal of Medicine, 2023. **388**(25). p. 2305-2308. Available from: https://doi.org/10.1056/NEJMp2305081.
101. *COVID Origins Hearing Wrap Up: Facts, Science, Evidence Point to a Wuhan Lab Leak*. United States House of Representatives, Committee on Oversight and Accountability, Select Subcommittee on the Coronavirus Pandemic. 2023. Available from: https://oversight.house.gov/release/covid-origins-hearing-wrap-up-facts-science-evidence-point-to-a-wuhan-lab-leak.
102. Pagani, I., et al., *Origin and evolution of SARS-CoV-2.* Eur Phys J Plus, 2023. **138**(2). p. 157.

103. Rissman, T. and A. Prieto. *Attributing Biological Weapons Use: Strengthening Department of Defense Capabilities to Investigate Deliberate Biological Incidents*. RAND Corporation. 2024. Available from: https://www.rand.org/pubs/research_reports/RRA2360-1.html.
104. Kuiper, I., *Microbial forensics: next-generation sequencing as catalyst: The use of new sequencing technologies to analyze whole microbial communities could become a powerful tool for forensic and criminal investigations.* EMBO Rep, 2016. **17**(8). p. 1085-7.
105. Oliveira, M. and A. Amorim, *Microbial forensics: new breakthroughs and future prospects.* Appl Microbiol Biotechnol, 2018. **102**(24). p. 10377-10391.
106. Budowle, B., S.E. Schutzer, and S.A. Morse, *Microbial forensics*. Third edition. ed. 2020, London, United Kingdom ; San Diego, CA: Academic Press, an imprint of Elsevier.
107. Bakerlee, C., et al. *Common Misconceptions About Biological Weapons*. Council on Strategic Risks. 2020. Available from: https://councilonstrategicrisks.org/wp-content/uploads/2020/12/Common-Misconceptions-About-Biological-Weapons_BRIEFER-12_2020_12_7.pdf.
108. English, E., *Can a 1975 bioweapons ban handle today's biothreats?* Bulletin of the Atomic Scientists, 2023. Available from: https://thebulletin.org/2023/03/biological-weapons-convention.
109. *China delayed releasing coronavirus info, frustrating WHO*. PBS News Hour. 2020. Available from: https://www.pbs.org/newshour/health/china-delayed-releasing-coronavirus-info-frustrating-who.
110. Stenseth, N.C., et al., *Lessons Learnt From the COVID-19 Pandemic.* Front Public Health, 2021. **9**: p. 694705.
111. Khanna, R.C., et al., *COVID-19 pandemic: Lessons learned and future directions.* Indian J Ophthalmol, 2020. **68**(5). p. 703-710.
112. Narayanasamy, S., et al., *Lessons From COVID-19 for Pandemic Preparedness: Proceedings From a Multistakeholder Think Tank.* Clin Infect Dis, 2023. **77**(12). p. 1635-1643.
113. Gormley, D.M., *Missile contagion : cruise missile proliferation and the threat to international security*. First Naval Institute Press Paperback ed. 2010, Annapolis, MD: Naval Institute Press.
114. Larsen, P.O. and M. von Ins, *The rate of growth in scientific publication and the decline in coverage provided by Science Citation Index.* Scientometrics, 2010. **84**(3). p. 575-603.
115. Williams, M., et al., *Summary of fourth annual MCBK public meeting: Mobilizing computable biomedical knowledge-metadata and trust.* Learn Health Syst, 2022. **6**(1). p. e10301.
116. Sacchi, L. and J.H. Holmes, *Progress in Biomedical Knowledge Discovery: A 25-year Retrospective.* Yearb Med Inform, 2016. **Suppl 1**(Suppl 1). p. S117-29.
117. Bornmann, L., R. Haunschild, and R. Mutz, *Growth rates of modern science: a latent piecewise growth curve approach to model publication numbers from established and new literature databases.* Humanities and Social Sciences Communications, 2021. **8**(1). p. 224. Available from: https://doi.org/10.1057/s41599-021-00903-w.
118. *Biotechnology Market Size, Share, Growth, Forecast 2024-2033*. Precedence Research. 2024. Available from: https://www.precedenceresearch.com/biotechnology-market.
119. Clarivate. *Clarivate Web of Science*. 2024. Available from: http://wokinfo.com/products_tools/multidisciplinary/webofscience/cpci/?parentKey=555184,539593.
120. Satam, H., et al., *Next-Generation Sequencing Technology: Current Trends and Advancements.* Biology (Basel), 2023. **12**(7).
121. Khalil, A.M., *The genome editing revolution: review.* J Genet Eng Biotechnol, 2020. **18**(1). p. 68.
122. van der Oost, J. and C. Patinios, *The genome editing revolution.* Trends Biotechnol, 2023. **41**(3). p. 396-409.

123. Wang, J.Y. and J.A. Doudna, *CRISPR technology: A decade of genome editing is only the beginning.* Science, **379**(6629). p. eadd8643. Available from: https://doi.org/10.1126/science.add8643.
124. Jinek, M., et al., *A programmable dual-RNA-guided DNA endonuclease in adaptive bacterial immunity.* Science, 2012. **337**(6096). p. 816-21.
125. Hawsawi, Y.M., et al., *The State-of-the-Art of Gene Editing and its Application to Viral Infections and Diseases Including COVID-19.* Front Cell Infect Microbiol, 2022. **12**: p. 869889.
126. Wickiser, J., et al., *Engineered Pathogens and Unnatural Biological Weapons: The Future Threat of Synthetic Biology.* CTC Sentinel: Combating Terrorism Center at West Point, 2020. **13**(8). Available from: https://ctc.westpoint.edu/engineered-pathogens-and-unnatural-biological-weapons-the-future-threat-of-synthetic-biology.
127. DiEuliis, D., et al., *Does Biotechnology Pose New Catastrophic Risks?* Curr Top Microbiol Immunol, 2019. **424**: p. 107-119.
128. Watters, K.E., et al., *The CRISPR revolution and its potential impact on global health security.* Pathog Glob Health, 2021. **115**(2). p. 80-92.
129. Berger, K.M. and P.A. Schneck, *National and Transnational Security Implications of Asymmetric Access to and Use of Biological Data.* Front Bioeng Biotechnol, 2019. **7**: p. 21.
130. Trump, B., et al., *Governing biotechnology to provide safety and security and address ethical, legal, and social implications.* Front Genet, 2022. **13**: p. 1052371.
131. Sleator, R.D., *Ferretting out the facts behind the H5N1 controversy.* Bioeng Bugs, 2012. **3**(3). p. 139-43.
132. Imai, M., et al., *Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5 HA/H1N1 virus in ferrets.* Nature, 2012. **486**(7403). p. 420-428. Available from: https://doi.org/10.1038/nature10831.
133. Herfst, S., et al., *Airborne Transmission of Influenza A/H5N1 Virus Between Ferrets.* Science, 2012. **336**(6088). p. 1534-1541. Available from: https://doi.org/10.1126/science.1213362.
134. Lipsitch, M., *Why Do Exceptionally Dangerous Gain-of-Function Experiments in Influenza?* Methods Mol Biol, 2018. **1836**: p. 589-608.
135. Cello, J., A.V. Paul, and E. Wimmer, *Chemical synthesis of poliovirus cDNA: generation of infectious virus in the absence of natural template.* Science, 2002. **297**(5583). p. 1016-8.
136. Noyce, R.S., S. Lederman, and D.H. Evans, *Construction of an infectious horsepox virus vaccine from chemically synthesized DNA fragments.* PLoS One, 2018. **13**(1). p. e0188453.
137. DiEuliis, D., K. Berger, and G. Gronvall, *Biosecurity Implications for the Synthesis of Horsepox, an Orthopoxvirus.* Health Secur, 2017. **15**(6). p. 629-637.
138. Paris, K., *Genome Editing and Biological Weapons: Assessing the Risk of Misuse*. 2022: Springer International Publishing. Available from: https://link.springer.com/book/10.1007/978-3-031-21820-0.
139. van Aken, J. and E. Hammond, *Genetic engineering and biological weapons. New technologies, desires and threats from biological research.* EMBO Rep, 2003. **4 Spec No**(Suppl 1). p. S57-60.
140. Kosal, M.E., *Emerging Life Sciences and Possible Threats to International Security.* Orbis, 2020. **64**(4). p. 599-614.
141. Noyce, R.S. and D.H. Evans, *Synthetic horsepox viruses and the continuing debate about dual use research.* PLoS Pathog, 2018. **14**(10). p. e1007025.
142. National Academies of Sciences, E., et al., *Biodefense in the Age of Synthetic Biology*. 2019: National Academies Press. Available from: https://www.ncbi.nlm.nih.gov/books/NBK535866/.
143. Koblentz, G.D. and R. Casagrande, *Beyond gain of function: strengthening oversight of research with potential pandemic pathogens.* Pathogens and Global Health: p. 1-12. Available from: https://doi.org/10.1080/20477724.2023.2265627.

144. Koblentz, G.D., *Dual-use research as a wicked problem.* Front Public Health, 2014. **2**: p. 113.
145. *Biosafety in Microbiological and Biomedical Laboratories, 6th Ed*. US Department of Health and Human Services, Centers for Disease Control and Prevention and National Institutes of Health. 2020. Available from: https://www.cdc.gov/labs/pdf/SF__19_308133-A_BMBL6_00-BOOK-WEB-final-3.pdf.
146. Koblentz, G. and F. Lentzos. *Global BioLabs Report 2023*. Global BioLabs. 2023. Available from: https://www.globalbiolabs.org/.
147. FinCEN. *Money Laundering Prevention: A Money Services Businesses Guide*. US Department of the Treasury, Financial Crimes Enforcement Network. 2023. Available from: https://www.fincen.gov/sites/default/files/shared/prevention_guide.pdf.
148. O'Brien, J.T. and C. Nelson, *Assessing the Risks Posed by the Convergence of Artificial Intelligence and Biotechnology.* Health Secur, 2020. **18**(3). p. 219-227.
149. AINow, *Computational Power and AI.* AI Now Institute, 2023. Available from: https://ainowinstitute.org/publication/policy/compute-and-ai.
150. Urbina, F., et al., *Dual use of artificial-intelligence-powered drug discovery.* Nature Machine Intelligence, 2022. **4**(3). p. 189-191. Available from: https://doi.org/10.1038/s42256-022-00465-9.
151. Urbina, F., et al., *Preventing AI From Creating Biochemical Threats.* Journal of Chemical Information and Modeling, 2023. **63**(3). p. 691-694. Available from: https://doi.org/10.1021/acs.jcim.2c01616.
152. Urbina, F., et al., *MegaSyn: Integrating Generative Molecular Design, Automated Analog Designer, and Synthetic Viability Prediction.* ACS Omega, 2022. **7**(22). p. 18699-18713.
153. Wang, S., et al., *DeepSA: a deep-learning driven predictor of compound synthesis accessibility.* Journal of Cheminformatics, 2023. **15**(1). p. 103. Available from: https://doi.org/10.1186/s13321-023-00771-3.
154. Bran, A.M., et al., *Chemcrow: Augmenting large-language models with chemistry tools.* arXiv preprint arXiv:2304.05376, 2023.
155. Carter, S., et al. *The Convergence of Artificial Intelligence and the Life Sciences*. Nuclear Threat Initiative. 2023. Available from: https://www.nti.org/wp-content/uploads/2023/10/NTIBIO_AI_FINAL.pdf.
156. Jumper, J., et al., *Highly accurate protein structure prediction with AlphaFold.* Nature, 2021. **596**(7873). p. 583-589.
157. Sawaya, S., T. Kuru, and T. Campbell. *The Potential for Dual-Use of Protein-Folding Prediction*. The Past, Present, and the Future...In Our Hands! Chemical, biological, radiological, and nuclear risk mitigation. Freedom From Fear Magazine. UNICRI. 2021. Available from: https://unicri.it/sites/default/files/2021-12/21_dual_use.pdf.
158. Thadani, N.N., et al., *Learning from prepandemic data to forecast viral escape.* Nature, 2023. **622**(7984). p. 818-825. Available from: https://doi.org/10.1038/s41586-023-06617-0.
159. Zhou, H., C. Astore, and J. Skolnick, *PHEVIR: an artificial intelligence algorithm that predicts the molecular role of pathogens in complex human diseases.* Scientific Reports, 2022. **12**(1). p. 20889. Available from: https://doi.org/10.1038/s41598-022-25412-x.
160. Soice, E.H., et al. *Can large language models democratize access to dual-use biotechnology?* 2023. Available from: https://arxiv.org/abs/2306.03809.
161. Mouton, C.A., C. Lucas, and E. Guest. *The Operational Risks of AI in Large-Scale Biological Attacks: Results of a Red-Team Study*. 2024. Available from: https://www.rand.org/pubs/research_reports/RRA2977-2.html.

162. *Oversight of A.I.: Principles for Regulation*. United States Senate Committee on the Judiciary. 2023. Available from: https://www.judiciary.senate.gov/committee-activity/hearings/oversight-of-ai-principles-for-regulation.
163. Anthropic. *Frontier Threats Red Teaming for AI Safety*. 2023. Available from: https://www.anthropic.com/news/frontier-threats-red-teaming-for-ai-safety.
164. Chowell, G., et al., *Real-time forecasting of epidemic trajectories using computational dynamic ensembles.* Epidemics, 2020. **30**: p. 100379. Available from: https://www.sciencedirect.com/science/article/pii/S1755436519301112.
165. Lmater, M.A., et al., *Modelization of Covid-19 pandemic spreading: A machine learning forecasting with relaxation scenarios of countermeasures.* J Infect Public Health, 2021. **14**(4). p. 468-473.
166. Jamshidi, M.B., et al. *A Review of the Potential of Artificial Intelligence Approaches to Forecasting COVID-19 Spreading*. AI, 2022. **3**, 493-511.
167. Kamalov, F., et al., *Deep learning for Covid-19 forecasting: State-of-the-art review.* Neurocomputing, 2022. **511**: p. 142-154. Available from: https://www.sciencedirect.com/science/article/pii/S0925231222010918.
168. Xu, L., R. Magar, and A. Barati Farimani, *Forecasting COVID-19 new cases using deep learning methods.* Comput Biol Med, 2022. **144**: p. 105342.
169. Saurabh, P., M. Parisa, and F. Amir Barati, *Forecasting COVID-19 New Cases Using Transformer Deep Learning Model.* medRxiv, 2023. p. 2023.11.02.23297976. Available from: http://medrxiv.org/content/early/2023/11/03/2023.11.02.23297976.abstract.
170. Yenurkar, G. and S. Mal, *Future forecasting prediction of Covid-19 using hybrid deep learning algorithm.* Multimed Tools Appl, 2023. **82**(15). p. 22497-22523.
171. Payedimarri, A.B., et al., *Prediction Models for Public Health Containment Measures on COVID-19 Using Artificial Intelligence and Machine Learning: A Systematic Review.* Int J Environ Res Public Health, 2021. **18**(9).
172. Duprex, W.P., et al., *Gain-of-function experiments: time for a real debate.* Nat Rev Microbiol, 2015. **13**(1). p. 58-64.
173. Shinomiya, N., et al., *Reconsidering the need for gain-of-function research on enhanced potential pandemic pathogens in the post-COVID-19 era.* Front Bioeng Biotechnol, 2022. **10**: p. 966586.
174. Thevenon, A., F. Sharples, and J. Husbands. *Gain-of-Function Research: Summary of the Second Symposium, March 10-11, 2016*. National Academies of Sciences, Engineering, and Medicine. 2016. Available from: https://www.ncbi.nlm.nih.gov/books/NBK373317/.
175. Selgelid, M.J., *Gain-of-Function Research: Ethical Analysis.* Sci Eng Ethics, 2016. **22**(4). p. 923-964.
176. Sharples, F.E., et al., *Potential risks and benefits of gain-of-function research : summary of a workshop*. 2015, Washington, D.C.: The National Academies Press. Available from: National Academies Press http://www.nap.edu/openbook.php?record_id=21666.
177. Nicholas Greig, E., L. Marc, and L. Meira, *The ethics of biosafety considerations in gain-of-function research resulting in the creation of potential pandemic pathogens.* Journal of Medical Ethics, 2015. **41**(11). p. 901. Available from: http://jme.bmj.com/content/41/11/901.abstract.
178. CRS. *Oversight of Gain of Function Research with Pathogens: Issues for Congress*. Congressional Research Service. 2022. Available from: https://crsreports.congress.gov/product/pdf/R/R47114.
179. HHS. *U.S. Government Gain-of-Function Deliberative Process and Research Funding Pause on Selected Gain-of-Function Research Involving Influenza, MERS, and SARS Viruses*. US Department of Health and Human Services. 2014. Available from: https://www.phe.gov/s3/dualuse/documents/gain-of-function.pdf.
180. Burki, T., *Ban on gain-of-function studies ends.* Lancet Infect Dis, 2018. **18**(2). p. 148-149.

181. *Proposed Biosecurity Oversight Framework fo the Future of Science*. National cience Advisory Board for Biosecurity. 2023. Available from: https://osp.od.nih.gov/wp-content/uploads/2023/03/NSABB-Final-Report-Proposed-Biosecurity-Oversight-Framework-for-the-Future-of-Science.pdf.
182. Schuerger, C., et al. *Understanding the Global Gain-of-Function Research Landscape*. Center for Security and Emerging Technology. 2023. Available from: https://cset.georgetown.edu/wp-content/uploads/20220035_Gain-of-Function-Research_FINAL.pdf.
183. *Strengthening Health Security Across the Globe: Progress and Impact of U.S. Government Investments in Global Health Security*. The White House. 2022. Available from: https://www.whitehouse.gov/wp-content/uploads/2023/12/Strengthening-Health-Security-Across-the-Globe.pdf.
184. Blinken, A.J. and X. Becerra, *Strengthening Global Health Security and Reforming the International Health Regulations: Making the World Safer From Future Pandemics.* JAMA, 2021. **326**(13). p. 1255-1256. Available from: https://doi.org/10.1001/jama.2021.15611.
185. Alilio, M., et al., *Strategies to Promote Health System Strengthening and Global Health Security at the Subnational Level in a World Changed by COVID-19.* Glob Health Sci Pract, 2022. **10**(2).
186. WHO. *WHO benchmarks for strengthening health emergency capacities* World Health Organization. 2024. Available from: https://iris.who.int/bitstream/handle/10665/375815/9789240086760-eng.pdf.
187. UN. *Goal 3: Good health and well-being - The Global Goals*. United Nations, Sustainable Development Goals. 2024. Available from: https://www.globalgoals.org/goals/3-good-health-and-well-being.
188. WHO. *Core Priorities: Protecting against health emergencies*. World Health Organization. 2024. Available from: https://www.who.int/europe/about-us/our-work/core-priorities/protecting-against-health-emergencies.
189. *One Health Initiative*. 2023. Available from: https://onehealthinitiative.com.
190. Marani, M., et al., *Intensity and frequency of extreme novel epidemics.* Proceedings of the National Academy of Sciences, 2021. **118**(35). p. e2105482118. Available from: https://www.pnas.org/doi/abs/10.1073/pnas.2105482118.
191. Carlson, C.J., et al., *Climate change increases cross-species viral transmission risk.* Nature, 2022. **607**(7919). p. 555-562. Available from: https://doi.org/10.1038/s41586-022-04788-w.
192. Semenza, J.C., J. Rocklöv, and K.L. Ebi, *Climate Change and Cascading Risks from Infectious Disease.* Infect Dis Ther, 2022. **11**(4). p. 1371-1390.
193. Grobusch, L.C. and M.P. Grobusch, *A hot topic at the environment-health nexus: investigating the impact of climate change on infectious diseases.* Int J Infect Dis, 2022. **116**: p. 7-9.
194. Lustgarten, A. *How Climate Change Is Contributing to Skyrocketing Rates of Infectious Disease*. ProPublica. 2024. Available from: https://www.propublica.org/article/climate-infectious-diseases.
195. Vidal, J. *Fevered Planet: How a shifting climate is catalysing infectious disease*. BBC. 2023. Available from: https://www.bbc.com/future/article/20231201-fevered-planet-how-climate-change-spreads-infectious-disease.
196. Teirstein, Z. *Warming planet may have overwhelming impact on infectious diseases*. PBS News Hour. 2023. Available from: https://www.pbs.org/newshour/science/warming-planet-may-have-overwhelming-impact-on-infectious-diseases.
197. Yong, E. *We Created the 'Pandemicene'*. The Atlantic. 2022. Available from: https://www.theatlantic.com/science/archive/2022/04/how-climate-change-impacts-pandemics/629699.

198. Leal Filho, W., et al., *Climate Change and Zoonoses: A Review of Concepts, Definitions, and Bibliometrics.* Int J Environ Res Public Health, 2022. **19**(2).
199. P Aki, p. *A warming world could unleash dangerous new pathogens. Metagenomics early warning tools are vital for pandemic prevention*. Atlantic Council. 2023. Available from: https://www.atlanticcouncil.org/blogs/new-atlanticist/a-warming-world-could-unleash-dangerous-new-pathogens-metagenomics-early-warning-tools-are-vital-for-pandemic-prevention.
200. Neumann, G. and Y. Kawaoka, *Which Virus Will Cause the Next Pandemic?* Viruses, 2023. **15**(1).
201. Marie, V. and M.L. Gordon, *The (Re-)Emergence and Spread of Viral Zoonotic Disease: A Perfect Storm of Human Ingenuity and Stupidity.* Viruses, 2023. **15**(8).
202. Mishra, C., et al., *Increasing risks for emerging infectious diseases within a rapidly changing High Asia.* Ambio, 2022. **51**(3). p. 494-507. Available from: https://doi.org/10.1007/s13280-021-01599-7.
203. Ellwanger, J.H. and J.A.B. Chies, *Zoonotic spillover: Understanding basic aspects for better prevention.* Genet Mol Biol, 2021. **44**(1 Suppl 1). p. e20200355.
204. *World Migration Report 2022*. International Organization for Migration. 2021. Available from: https://publications.iom.int/books/world-migration-report-2022.
205. *OECD International Migration Outlook 2023*. Organisation for Economic Co-operation and Development. 2024. Available from: https://www.oecd.org/migration/international-migration-outlook-1999124x.htm.
206. Tang, J.W., et al., *An exploration of the political, social, economic and cultural factors affecting how different global regions initially reacted to the COVID-19 pandemic.* Interface Focus, 2022. **12**(2). p. 20210079.
207. WHO. *Chapter 3: Factors that contributed to undetected spread of the Ebola virus and impeded rapid containment*. in One year into the Ebola epidemic. January 2015. World Health Organization. 2015. Available from: https://www.who.int/news-room/spotlight/one-year-into-the-ebola-epidemic/factors-that-contributed-to-undetected-spread-of-the-ebola-virus-and-impeded-rapid-containment.
208. Allinder, S.M., *Barriers to Control of South Africa's HIV Epidemic*, in *South Africa's Future at the Brink*. 2020, Center for Strategic and International Studies (CSIS). p. 9-24.
209. Wang, J. and L. Qi. *WHO Says China Is Undercounting Covid Deaths, Asks for More Reliable Data*. The Wall Street Journal. 2023. Available from: https://www.wsj.com/articles/who-prods-china-to-release-reliable-covid-19-data-11672862046.
210. Ding, C., *Fatal Lack of Information Transparency in Public Health Emergency: Lessons from the COVID-19 Outbreak in China.* Hong Kong Law Journal, 2020. **50**(2). p. 781-808. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3715380.
211. Brennan, M. *State Department says coronavirus samples from China "critical" for developing vaccine; Experts say that's not the case*. CBS News. 2020. Available from: https://www.cbsnews.com/news/state-department-says-coronavirus-samples-from-china-critical-for-developing-vaccine-experts-say-thats-not-the-case.
212. Roberts, G.B., *Arms Control without Arms Control: The Failure of the Biological Weapons Convention Protocol and a New Paradigm for Fighting the Threat of Biological Weapons*, U.I.f.N.S. Studies, Editor. 2003.
213. Gerstein, D. and J. Giordano, *Rethinking the Biological and Toxin Weapons Convention?* Health Secur, 2017. **15**(6). p. 638-641.
214. Revill, J. *Compliance Revisited: An Incremental Approach to Compliance in the Biological and Toxin Weapons Convention*. Middlebury Institute of International Studies at Monterey, James

Martin Center for Nonproliferation Studies. 2017. Available from: https://www.nonproliferation.org/wp-content/uploads/2017/08/op31-compliance-revisited.pdf.
215. *Use of Chemical, Biological Weapons Unacceptable in Any Context, Delegates Stress, as First Committee Continues General Debate | Meetings Coverage and Press Releases*. United Nations, Seventy-Sixth Session, 5th Meeting. 2021. Available from: https://press.un.org/en/2021/gadis3666.doc.htm.
216. Zanders, J.P., *International Norms Against Chemical and Biological Warfare: An Ambiguous Legacy.* Journal of Conflict & Security Law, 2003. **8**(2). p. 391-410. Available from: http://www.jstor.org.mutex.gmu.edu/stable/26294282.
217. Kirby, J. *Why arms control is getting harder — but still really matters*. Vox Media. 2023. Available from: https://www.vox.com/world/23510633/arms-control-bioweapons-convention-nukes-ukraine-putin.
218. Khan, S. *Norms Against Bioweapons Use Are Unraveling*. Inkstick Media. 2023. Available from: https://inkstickmedia.com/norms-against-bioweapons-use-are-unraveling.
219. Leitenberg, M. *Assessing the Biological Weapons and Bioterrorism Threat*. US Army War College Press. 2005. Available from: https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1029&context=monographs.
220. Mir, T.u.G., et al., *Microbial forensics: A potential tool for investigation and response to bioterrorism.* Health Sciences Review, 2022. **5**: p. 100068. Available from: https://www.sciencedirect.com/science/article/pii/S2772632022000563.
221. Bidwell, C.A. and K. Bhatt *Use of Attribution and Forensic Science in Addressing Biological Weapon Threats: A Multi-Faceted Study*. 2016.
222. *2022 Country Reports on Human Rights Practices*. United States Department of State. 2022. Available from: https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/.
223. Naimark, N.M., *Genocide : a world history*. The New Oxford world history. 2017, New York, NY: Oxford University Press.
224. Juling, D., *Future Bioterror and Biowarfare Threats for NATO's Armed Forces until 2030.* Journal of Advanced Military Studies, Vol 1, No 14, 2023. Available from: https://www.usmcu.edu/Portals/218/JAMS%2014_1_Spring2023_Juling.pdf.
225. Gregory, K., *Pathogens as Weapons: The International Security Implications of Biological Warfare.* International Security, 2003. **28**(3). p. 84-122. Available from: http://www.jstor.org.mutex.gmu.edu/stable/4137478.
226. Markov, P.V., et al., *The evolution of SARS-CoV-2.* Nature Reviews Microbiology, 2023. **21**(6). p. 361-379. Available from: https://doi.org/10.1038/s41579-023-00878-2.