COUNCIL ON STRATEGIC RISKS

THE NOLAN CENTER

BRIEFER

No. 18 | May 3, 2021

Weapons of Mass Agility: A New Threat Framework for Mass Effects in the 21st Century

Natasha E. Bajema

Introduction

The threat posed by weapons of mass destruction (WMD) continues to serve as a key concept for shaping U.S. national security strategy. For many decades, policymakers and experts alike have assumed that malicious actors will seek WMD for their potential to cause mass casualties and destruction. And yet, the historical record of use cases for chemical, biological, radiological, and nuclear weapons (CBRN) over the past three decades is not consistent with their designation as weapons of "mass destruction." While their potential for mass destruction remains catastrophic, most WMD attacks have involved the use of chemical, biological, or radiological materials for targeting individuals (e.g., assassinations) or to produce targeted casualties in specific populations (e.g., tactical use of chemical agents). Additionally, the world has seen significant political, technological, and structural changes since the concept of WMD focused specifically on CBRN in U.S. national security strategy.[1]

[1] See Natasha E. Bajema, *Beyond Weapons of Mass Destruction: Time for a New Paradigm?* Washington D.C.: The Council on Strategic Risks, 2021; Natasha E. Bajema, *Definitions Matter: The Role of WMD in Shaping U.S. National Security Strategy*, Washington D.C.: The Council on Strategic Risks, 2021.

The current technological landscape is generating many new scenarios capable of causing mass effects, which arise from the complexities of the digital and modern world. New technologies such as drone swarms and cyber weapons have the potential to rise to the level of a notional WMD. The convergence of multiple technologies in unexpected ways could generate high levels of destruction and casualties.

Nefarious actors seeking to cause mass effects are likely to consider a broader range of options for achieving their goals rather than seeking WMD in isolation.[2] Over the past three decades, most actors appear to be using WMD for deterrence and to capitalize on their disproportionate psychological effects and their significant advantage of mass publicity. As they are currently defined, the emphasis on WMD in U.S. national security not only misses important gaps in the mass effect threat spectrum, it fails to examine the increasing use of CBRN at the lower end of that spectrum.

What makes a weapon of mass destruction a WMD? What are the criteria for designating a potential weapon as such? Despite the relative importance of WMD to U.S. national security policy, there are no satisfying answers to these questions. The specific characteristics of a WMD have not been adequately debated among policymakers in past decades. Meanwhile the designation of a weapon as WMD conveys major policy implications. As discussed in the first briefer in this series, the recent debate on whether or not fentanyls constitute WMD demonstrates just how outdated the boundaries for consideration are within the U.S. government.

U.S. policymakers need a better way to consider and prioritize emerging threats with mass effects potential in the 21st century.

The challenge of rethinking U.S. national security priorities on a grand scale can be daunting, especially when new threats with potential for mass effects are more complex, diffuse, and interconnected with the civilian world. The task involves making decisions on what things to include, what things to exclude, and having a decent rationale to support both types of decisions. A valid fear exists among U.S. policymakers that consideration of new technologies and scenarios would clutter the "tidy WMD box" or possibly diminish the importance of CBRN relative to other threats. There are concerns that any redrawing of such boundaries is akin to opening Pandora's box; that by considering new technologies and scenarios, we run the risk of diluting the important mission set of countering CBRN.

However, if we do not think outside the box and beyond the WMD paradigm and fail to take into account the new features of today's security environment, we run an even greater risk—a failure of imagination of the kind that preceded the 9/11 attacks. U.S. policymakers need a new framework for thinking more broadly about weapons of mass effects and assessing priorities across all technologies and scenarios that could cause great harm to people and infrastructure, both domestically and overseas.

---

[2] William C. Yengst, "Next Generation Weapons of Mass Effect," in Lewis A. Dunn et al, *Next Generation Weapons of Mass Destruction and Weapons of Mass Effects Terrorism*, January 2008, Advanced Systems and Concepts Office, Defense Threat Reduction Agency, Report Number ASCO 2008 001.

This briefer is the third part of a series in which I deconstruct the concept of WMD and its influential role in shaping U.S. national security policy and discuss the urgent need for consideration of new types of threats. In this briefer, I propose a new concept of "weapons of mass agility"—i.e., weapons that have the potential to cause mass effects, but also can be used at the lower end of the casualty and destruction spectrum to exploit their significant strategic impact. This concept opens the aperture to technologies and scenarios with mass effect potential while empowering policymakers to more creatively and effectively address the trend in CBRN use at the lower end of the mass effect spectrum. I also propose a framework and a set of criteria for determining technologies and scenarios with mass effects potential, including CBRN, and assigning relative priority to them.

The Need to Adapt to the Changing Technological Context

In recent years, the technological context has changed dramatically, revealing gaps in U.S. national security strategy when it comes to dealing with threats of mass effects. A new framework would take several significant changes in the threat environment into account.

CBRN were designated as the first WMD because of their obvious potential for causing mass destruction and casualties. It has always been assumed that states and violent non-state actors would be interested in CBRN primarily for their ability to cause mass harm. However, over the past three decades, CBRN have been used more often by state actors for their strategic impact rather than their potential for mass effects, as illustrated by the Novichok and VX nerve agent assassination cases. This trend possibly indicates a modern preference by state actors to use these weapons in a discriminate manner. CBRN may offer attractive methods for assassinations and other tailored uses because they flout accepted norms and send a strong, in-your-face message by states that use them. Recent advances in biotechnology and gene editing techniques may increase this trend in the future. There is growing potential for creating biological weapons designed to affect highly specific targets, assisted by greater availability of genomic and health data and better understanding of gene functions.

In a profound technological shift, the boundaries between the physical and digital worlds have blurred. This trend challenges the current utility of separating cyber and CBRN into different bureaucratic silos.[3] Increasing connectedness between digital systems and elements of the physical world has made gray zone actions by states more attractive. Unlike CBRN, cyberweapons have not yet encountered an international taboo despite their potential for mass effects. Cyberweapons are far more accessible than CBRN to a broader range of actors, given the widespread availability of open source scripts and other online tools. Such attacks are also scalable, capable of producing both outcomes at the lower end of the mass effect spectrum and much more devastating results. Both states and violent non-state actors may resort to using cyberweapons as an alternative to CBRN or select an innovative combination between them in order to achieve mass effects in the future.

Nefarious actors, intent on using CBRN, may turn to digital pathways and leverage convergence across new technologies to achieve the element of surprise. Through interaction with emerging

[3] Natasha E. Bajema, "Countering WMD in the Digital Age: Breaking Down Bureaucratic Silos in a Brave New World," *War on the Rocks*, 13 May 2019.

technologies, the CBRN threat may increasingly exhibit digital elements in the future, allowing actors new ways to develop and use CBRN and avoid detection.[4] For example, drones, potential platforms for the remote delivery of CBRN, contain operating software and hardware, transmit many types of data, and rely upon GPS for navigation. Drones could allow for the launch of CBRN attacks from remote locations, the origins of which may be difficult to trace. As another example, 3D printers could allow nefarious actors to reverse engineer and produce CBRN-related parts, avoiding purchases from traditional suppliers that could tip off export controllers and reducing their chance of detection.

This new phenomenon is most evident in the "digitization of biology." This refers to the ability to translate DNA into digital information through gene sequencing and back into physical DNA through gene synthesis.[5] Today, nefarious actors no longer need a physical sample of a dangerous virus to develop biological weapons. Rather, with some technical expertise and access to online genomic data, they could acquire the genome and then recreate the pathogen through easily acquired materials in a lab. The current WMD paradigm treats CBRN as a physical problem, completely distinct from cyber, creating a gap in U.S. national security strategy.

Adding to the complexity in today's security environment, the increased connectedness of U.S. society over social media channels and the Internet of Things could also help amplify the second and third order effects of both CBRN and non-CBRN attacks by states and violent non-state actors—especially if combined with disinformation campaigns.[6] Such amplification could cause a lower impact scenario to spiral out of control and lead to disproportionate effects. This enabling feature of the digital world suggests that a broader range of technologies and scenarios could cause mass effects and become attractive options for actors seeking to cause harm to significant numbers of people.[7]

Finally, the private sector is currently leading the development of advanced technologies with potential military applications, representing a significant departure from the past. In the past, advanced technologies like those supporting CBRN were developed first for military use within the defense sector and then transferred to the private sector for relevant civilian applications. The trend toward private sector leadership on tech development has arisen due to low barriers for entry, widespread availability on open markets, cheap open source solutions, and the rapid pace of technological advancement.[8] New technologies that pose national security risks often now start out as civilian technologies in the private sector. They are thus more accessible and easier to use than CBRN. They can introduce new types of security risks, for example the concern of

---

[4] See Natasha E. Bajema, *WMD in the Digital Age: Understanding the Impact of Emerging Technologies*, Washington D.C.: National Defense University, 2018.

[5] See Natasha E. Bajema, Diane DiEuliis, Charles Lutes, and Yong-Bee Lim, *The Digitization of Biology: Understanding the New Risks and Implications for Governance*, Washington D.C.: National Defense University, 2018.

[6] James Andrew Lewis, *Reconsidering Cybersecurity: Strategy, Mass Effect, and States*, Washington D.C.: CSIS, 2018, 22.

[7] James Andrew Lewis, *Reconsidering Cybersecurity: Strategy, Mass Effect, and States*.

[8] See Natasha E. Bajema, *WMD in the Digital Age: Understanding the Impact of Emerging Technologies*; See also Natasha E. Bajema, *The Future of Defense Innovation: Removing the Silos between Warfighters and Innovators*, Washington D.C.: National Defense University, 2018.

nefarious offensive uses of gain of function research conducted by civilian scientists to learn how to potentially enhance certain attributes of viruses, such as making them more transmissible in humans. As the number and range of stakeholders with access to technologies with military relevance increases, so does the potential for nefarious actors to cause significant harmful effects with technologies other than CBRN.

Given the bureaucratic institutionalization of WMD as a key concept in U.S. national security strategy over many decades, it has become increasingly difficult to think outside the box and consider the mass effect potential of new technologies and scenarios. Yet the need to do so is pressing.

What is a Weapon of Mass Destruction (WMD)?

Before proposing a new framework that includes CBRN and a full range of other technologies and scenarios capable of producing mass effects across a wide spectrum of destruction and casualties, it is necessary to first examine the boundaries of the WMD paradigm: what are the specific characteristics that define a WMD?

The term "weapons of mass destruction" originated during a specific historical context.[9] In 1948, the United Nations Commission on Conventional Armaments (CCA) defined WMD for the first time as "atomic explosive weapons, radioactive material weapons, lethal chemical and biological weapons, and any weapons developed in the future which have characteristics comparable in destructive effect to those of the atomic bomb or other weapons mentioned above."[10] Importantly, the original definition of WMD explicitly allowed for consideration of weapons based on new scientific principles with similar characteristics.[11]

As discussed in the second briefer in this series, in practical use, the term WMD has become synonymous with chemical, biological, radiological, and nuclear weapons (CBRN). Consequently, despite early intentions for the WMD categorization to be an evolving way to understand and address threats with mass effects, there is no existing framework for assessing new potential weapons or technologies for inclusion in the category of WMD.

What makes a weapon of mass destruction a WMD? What are the criteria for designating a potential weapon as such?

The two most common characteristics used to define WMD are mass casualties and mass destruction.[12] The Department of Defense includes two qualifiers to its definition, stipulating that WMD are "chemical, biological, radiological, or nuclear weapons capable of a high order of

---

[9] The term was first used in 1937 by William Cosmo Gordon Lang, the Archbishop of Canterbury, in his Christmas address. See W. Seth Carus, *Defining "Weapons of Mass Destruction*, Occasional Paper No. 8, Washington D.C.: National Defense University, 2012.

[10] Commission for Conventional Armaments, *Resolutions Adopted by the Commission at its Thirteenth Meeting*, 12 August 1948.

[11] W. Seth Carus, *Defining "Weapons of Mass Destruction,"* 21.

[12] W. Seth Carus, *Defining "Weapons of Mass Destruction."*

destruction or causing mass casualties."[13] These characteristics were intended to clarify why the U.S. places top priority on WMD; they are capable of significant damage and strategic impact. Even so, the two qualifiers fail to solve the ambiguity problem. They do not establish clear boundaries for determining what constitutes WMD and what does not, as the case of fentanyl suggests. There are about 130 deaths per day in the United States, costing the economy about $78.5 billion per year in health costs and loss of productivity.[14]

The required magnitude for "mass destruction" or the specific nature of such higher order destruction have not been further defined. The term "mass destruction" could be conceived broadly to include the physical destruction of buildings, any destruction related to contamination by CBRN, the crippling of key infrastructure such as the public health system or the financial system, and anything else that would harm U.S. capacity to respond and require some rehabilitation to return to normal operation.

In practice, however, the term "mass destruction" is assumed to refer to the kind of physical destruction such as that caused by the detonation of a nuclear weapon. But this narrowly drawn notion excludes most potential uses of chemical and biological weapons, which would not likely be delivered using an explosive device. Moreover, causing significant damage to property and infrastructure is not unique to the use of CBRN, and therefore not a useful defining feature for these weapons relative to others. Though the potential threat for a broad spectrum of uses of WMD remains, in nearly seven decades, there have been no WMD-related incidents on U.S. soil resulting in the level of significant physical destruction the current definition of WMD indicates—unless of course, decontamination efforts required by the anthrax letter attack in 2001 are considered to qualify.

The term "mass casualties"—i.e., number of injuries and deaths—suffers from similar problems given the absence of clearly specified and agreed upon parameters. The DoD defines mass casualties as "any number of human casualties produced across a period of time that exceeds available medical support capabilities."[15] This conception of mass casualties does not identify a clear threshold and depends inherently on the capacity of the target to absorb harm.

Other government agencies propose thresholds, but these are also not helpful for definitional purposes. The Department of Homeland Security defines the threshold for a mass casualty event as 1,000 casualties or more, but only a handful of incidents in recent decades come close to this number.[16] The Department of Health and Human Services defines its mass casualty threshold based on the capacity of the public health system for handling patients. In this case, a mass casualty event would generate "many more patients at one time than locally or regionally available resources can manage using routine emergency procedures."[17] However, the number of

---

[13] *DoD Dictionary of Military and Associated Terms*, June 2019; See also *Countering Weapons of Mass Destruction*, Joint Publication 3-40, 31 October 2014.

[14] National Institute on Drug Abuse; U.S. Department of Health and Human Services.

[15] *DoD Dictionary of Military and Associated Terms.*

[16] U.S. Government Accountability Office, *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments for Chemical and Biological Attacks*, Washington D.C.: GAO, 1999.

[17] Centers for Medicare and Medicaid Services, "Mass Casualty Preparation."

patients that would overwhelm the public health system would vary significantly for a large city or small town. Similar to mass destruction, the number of casualties does not represent a defining feature for WMD, nor capture the strategic impact that more targeted uses could still have.

In practice, the designation of WMD appears arbitrary and dissociated from their actual effects. Novichoks are WMD because they were developed specifically for the battlefield, whereas fentanyls, though as lethal as chemical warfare agents, are not WMD under currently-used definitions. Moreover, attacks by states or violent non-state actors involving WMD-related materials—i.e., dangerous pathogens, toxic chemicals, and/or radioisotopes—are considered WMD even when they were not used to cause mass effects.

Weapons of Mass Agility: A New Concept and Framework

To facilitate decisions about prioritizing threats, U.S. policymakers need a new concept based on "weapons of mass agility" that encompasses both CBRN and other technologies and scenarios with the potential for mass effects. This briefer proposes a simple framework and a set of specific criteria for identifying technologies and scenarios with mass effects potential and assigning relative priority to them.

In significant contrast to CBRN, most emerging technologies and cybertools are not inherently dangerous to people or infrastructure; they exhibit neutrality until they are used in a specific scenario to achieve mass effects.[18] For example, a drone can be used to deliver critical blood supplies to remote locations, or it can be used to crash into a target and cause damage. Thus, the potential of emerging technologies and cyber tools for causing mass effects is less direct than CBRN. To accommodate these issues, a weapon of mass agility is defined as a technology or combination of technologies with the **potential to cause mass effects (1)** when delivered to and used on a target.[19]

Mass effects can involve a diverse range of consequences including casualties (injuries and fatalities), physical damage, disruption of or damage to infrastructure, political and psychological impacts, and/or economic damages. Not all types of mass effects are quantifiable or easily measured. A technology or scenario that does not have the potential to cause mass effects from the outset would not be considered as part of this framework (e.g., hacking servers to gain access to personal information). Of course, on its own, this criterium would generate a long and impossibly diverse list of scenarios. To further narrow the technologies and scenarios for consideration, this paper proposes several additional criteria.

Any scenario must involve the **malicious intent by a state or violent non-state actor (2)**. This metric narrows the field of potential scenarios by excluding accidents, natural disasters or outbreaks, and any unintentional consequences. A technology or scenario becomes a weapon when it is intentionally wielded as such.

[18] See Bajema, *WMD in the Digital Age: Understanding the Impact of Emerging Technologies.*

[19] Yengst, "Next Generation Weapons of Mass Effect."

A weapon of mass agility must be capable of achieving a major first order impact in at least one type of effect, but it must also have persistent impact and lead to **significant second and third order effects (3)**. As such, this framework excludes technologies and scenarios with significant first order effects such as mass shootings or the bombing of a single target, which though tragic and lethal, do not inherently lead to further waves of effects after the initial attack and response. Notably, first order casualties are not required for a weapon of mass agility. As such, this framework could include technologies or scenarios that lead to massive economic damages, such as the NotPetya attack.

A weapon of mass agility must have **minimal target dependency (4)**, which is a sliding spectrum rather than a well-defined metric; policymakers applying this framework could determine the appropriate boundary to limit the scope of what is included. Irrespective of weapon choice, the specific characteristics and vulnerability of a target always matter for achieving mass effects. Although choice of target plays an important role in mass effects scenarios, the weapon should not depend solely on the target's vulnerability for causing mass effects. If delivered or used against a target, both a nuclear weapon and a drone swarm carrying conventional explosives would reliably cause great harm to people, nature, and infrastructure. In other words, the target vulnerability does not vastly increase the initial potential of the weapon to cause mass effects. Depending on how this metric is applied, the framework could include or exclude the use of cyberattacks attempting to cause a meltdown at a nuclear power plant. The success of such an attack would rely inherently upon the target vulnerability. Unless all redundant safety measures failed simultaneously and a specified series of events took place at the target, the cyberweapon would not cause any mass effects and would therefore fall outside this framework.

A weapon of mass agility must achieve a **high density of effects (5)** across time and space, proportional to its mass, dose, and/or cost. There are several different facets to this metric: time, space, and proportionality. In terms of density across time, the first order effects should be fairly concentrated but do not have to be immediate. This takes into account relevant incubation periods following exposure to dangerous pathogens or toxins. This metric would exclude, however, longer-term scenarios such as disinformation campaigns, identity theft hacks, or other scenarios with multiple events taking place over a long period of time. The density of effects across space is a bit more complicated. A weapon of mass agility could produce a high volume of effects in a small area (concentrated) or a high volume of effects distributed across multiple areas (distributed). Thus, this framework would include an attack with a highly contagious pathogen that starts with a limited initial release.

For a weapon of mass agility, proportionality is important. A high density of effects must be achieved with a relatively low mass or dose proportional to the effects, or for some weapons types, a low cost to mass effects ratio. With the cost-to-effect ratio, this framework includes scenarios leveraging technologies that are more accessible and easier to use than CBRN but still capable of producing mass effects.

Finally, a weapon of mass agility involves a **fear factor (6)** that generates a psychological impact on the affected population and amplifies second and third order effects. A fear factor could result from the invisibility or uncertainty of physiological effects. For CBRN, exposure to

dangerous substances is often invisible, leading to a greater psychological and political impact when such weapons are used. However, fear may also stem from an inability to attribute an attack to the responsible actor or identify the source of the effects. The fear factor is a dynamic metric that directly relies upon what technologies or scenarios invoke great fear in a given population at a given time. Until cyberattacks cause more fear amongst the general public, most cyberattacks would need to be carried out at a scale and scope to meet the definitions above and qualify as weapons of mass agility.[20] However, a shift in the ratio of positive to negative effects associated with the Internet could enable cyber to have similar second and third order effects typically associated with CBRN.

This proposed framework is likely to generate a broader list of technologies and scenarios capable of causing mass effects than the WMD paradigm. For this reason, it is important that U.S. policymakers prioritize technologies and scenarios according to assessed threats by state and violent non-state actors, vulnerabilities of various targets, as well as the probability and range of potential mass effects.

Conclusion

The WMD paradigm has exceeded its utility for describing the top threats to U.S. national security. Until it is reconsidered, it will limit the ability of U.S. policymakers to effectively address new technologies and new trends, including in the use of CBRN. Consideration of new threats capable of producing mass effect does not have to diminish the priority assigned to preventing the proliferation, development, and use of CBRN. This briefer proposes a framework and a set of criteria for determining potential technologies and scenarios with mass effects potential, including CBRN, and assigning relative priority to them: 1) potential to cause mass effects; 2) malicious intent; 3) significant second and third order effects; 4) minimal target dependency; 5) high density of effects; and 6) a fear factor.

As a useful first step, the U.S. government should take up the topic and host interagency discussions to rethink the current threat environment and map out the most important threats of mass effect. Once U.S. policymakers agree on the list, they can prioritize technologies and scenarios according to threats by state and violent non-state actors, the vulnerabilities of various targets, as well as the probability and range of potential mass effects.

To avoid another failure of imagination akin to 9/11, U.S. policymakers should move beyond the WMD paradigm as an organizing principle and think more broadly about weapons of mass agility.

Dr. Natasha E. Bajema is the Director of the Converging Risks Lab at the Council on Strategic Risks (CSR) and a Senior Fellow at CSR's Janne E. Nolan Center on Strategic Weapons.

The author would like to thank Dr. W. Seth Carus for his many insights and extensive feedback in the writing of these briefers. The author would also like to thank Mr. Jim Stokes, Director of the CWMD Systems Program Office within the Department of Defense.

[20] Lewis, *Reconsidering Cybersecurity*, 23.