6-2021

Cyber Threats and Weapons of Mass Destruction

Shane Smith

Center for the Study of WMD Weapons of Mass Destruction
NATIONAL DEFENSE UNIVERSITY
wmdcenter.ndu.edu
PROCEEDINGS

Cyber Threats and Weapons of Mass Destruction

June 2021

By Shane Smith

At the 2020 WMD Center Symposium, General John E. Hyten, USAF, Vice Chairman of the Joint Chiefs of Staff, expressed a view that is widely shared in the U.S. strategic community: "A catastrophic attack from cyber could be looked at as a weapon of mass destruction."[1] For two decades, U.S. policymakers, military leaders, and analysts have drawn connections between cyber threats and WMD that demand attention from experts who work in both fields.

While recognizing there are a variety of definitions for WMD in use today, the WMD Center does not believe classifying cyber threats as WMD is warranted or advantageous for the United States at this time.[2] Canonically defined WMD (chemical, biological, radiological, and nuclear weapons [CBRN]) have the known potential to produce largescale lethal effects, whereas the lethality of cyber weapons remains largely unproved—a 2020 ransomware attack on a German hospital resulted in what may be the first confirmed fatality due to a cyber attack.[3]

Even in future scenarios in which cyber weapons prove to have lethal potential, there are reasons for caution about labeling them WMD.[4] Namely, cyber weapons' ability to create widespread loss of life or physical destruction stems primarily from the second- or third-order effects that may follow a catastrophic cyber attack on critical infrastructure, such as power grids, dams, or healthcare networks. A wide range of different types of attacks against critical infrastructure, however—including using conventional munitions or armed infiltration to manually disable key facilities—could achieve similar effects. There is no clear rationale for singling out cyber as WMD. Meanwhile, attaching the WMD moniker to cyber weapons could have negative legal, diplomatic, and operational implications for existing efforts to prevent and counter the spread of traditionally defined WMD.

Under international law, WMD carries special meaning as a category of weapon that is subject to control and outright elimination, whereas no consensus exists on whether or how to regulate cyber weapons. While the United Nations Conference on Disarmament "[r]eaffirms that effective measures should be taken to prevent the emergence of new types of weapons of mass destruction," it has never added a new type of weapon to this category and does not specify criteria for determining what type of weapon would qualify for WMD designation.[5] Relatedly, there may be compelling benefits for the United States to avoid international regulation of cyber weapons to the extent that it possesses advantages over adversaries in that domain.

Shane Smith is a Senior Policy Fellow in the Center for the Study of Weapons of Mass Destruction, Institute for National Strategic Studies, at the National Defense University. Special thanks to Samantha O. Arnett, Paul Bernstein, W. Seth Carus, John P. Caves, Jr., Diane DiEuliis, Gerald L. Epstein, Brendan Melley, Amy J. Nelson, and Patrick R. Terrell for insights and feedback on early drafts.

WMD also represent a limited problem set in terms of historical employment, perceived utility, and proliferation challenges. By contrast, cyber attacks are part of a spectrum of day-to-day competition, conflict, and crime by a growing number of actors with increasingly perceived utility against modern militaries and societies. Expanding the definition of WMD to include cyber weapons would make it exceedingly difficult to limit the scale and scope of WMD threats the U.S. Government prioritizes and against which it organizes to prevent and counter.

Also, the legal authorities, activities, programs, and capabilities for addressing currently defined WMD are associated to physical modalities—objects or substances that are conveyed to a target and then detonated or dispersed. Although they could have physical effects, cyber weapons do not have physical form. The ways in which such attacks are detected, analyzed, diagnosed, attributed, and countered are radically different from those needed for more traditional WMD.

While in and of themselves, cyber weapons are not WMD, there are five ways in which cyber and WMD intersect that merit new thinking and approaches to addressing threats where the two converge. One way aligns with General Hyten's statement: when future cyber attacks have the ability to create catastrophic consequences on an order of magnitude that is often associated with canonical WMD. Such threats could be considered strategic in their potential effects and thus national leaders may depend on deterrence measures that have historically been reserved for deterring WMD attacks. A second intersection is the growing concern that adversaries could use cyber weapons against nuclear or chemical plants to release radiation or toxins.[6] A third stems from the potential for adversaries to employ cyber attacks against nuclear command, control, and communication (NC3) systems in ways that make nuclear conflict more likely. Fourth, adversaries could use cyber weapons to better enable or amplify the consequences of a WMD attack. Last, cyber weapons could be valuable counterproliferation tools to disrupt or disable adversary WMD programs. What follows is a breakdown of these five intersections.

Cyber Weapons as a Strategic Capability

Modern militaries and societies, more broadly, are increasingly dependent on information technology to function effectively. This dependency makes them vulnerable to potentially catastrophic cyber attacks with strategic consequences not unlike what have been historically associated with WMD threats. For instance, experts increasingly warn about the cyber vulnerabilities of critical infrastructure, such as U.S. transportation services, the electrical grid, water and wastewater systems, public health, and food and pharmaceutical distribution networks.[7] A massive cyber attack that shuts down one of these systems for an extended period of time could wreak massive disruption on societal functions with potentially devasting costs. Such threats have not yet manifested, but they are not out of the realm of possibility.

To deter attacks of this kind, the United States and others might increasingly rely on measures that were once reserved for responding to a traditional WMD attack. In fact, debate is already well under way in the United States about whether to use nuclear weapons or the threat of "unacceptable costs" to deter strategic cyber attacks. The attention to cyber threats in the 2018 U.S. *Nuclear Posture Review* and debate resulting from the declaratory policy it established to deter "non-nuclear strategic attacks" is one illustration of the strategic connection between some cyber threats and nuclear deterrence that is growing in the minds of some in the U.S. policy community.[8]

Cyber Attacks on Nuclear Reactors and Chemical Plants

There is growing concern among many experts that adversaries could use cyber weapons to penetrate and manipulate the industrial control systems at nuclear or chemical plants, resulting in the release of radiation or toxins with Chernobyl- or Bhopal-like effects.[9] But such an induced release would not necessarily need to produce the level of mass casualties or widespread destruction that resulted in the former cases to have far-reaching political, economic, or social consequences. Radiological and chemical hazards have historically produced widespread dread within societies that confront them.

This type of threat is squarely in the realm of traditional notions of WMD because it involves the release of radiation or chemicals. However, it is the *effect* of such a release, and not its proximate cause, that matters most for the countering-WMD community. A cyber weapon in this kind of

scenario might be thought of as a delivery system, such as a missile. A missile is not a WMD threat, unless it is armed with a CBRN warhead/dispersal device. The countering-WMD community should be engaged in efforts to reduce, mitigate, and respond to threats against chemical or nuclear plants regardless of whether an attacker uses a cyber weapon, conventional explosives, or manually turns a valve to create the release of WMD material. The community has substantial background, expertise, and resources to contribute.

Cyber Attacks on Nuclear Systems

Recent reports highlight potential cyber vulnerabilities in the U.S. NC3 system that enables early warning, timely and deliberate decisionmaking, and the management of U.S. nuclear forces during crises.[10] Presumably those vulnerabilities are not unique to the United States: all nuclear-armed states likely face similar challenges. The possibility of a cyber attack on NC3 systems raises concern among some experts that such cyber attacks could weaken strategic deterrence and make nuclear conflict more likely. For instance, cyber attacks on its NC3 could lead the United States to doubt the surety of its deterrent and embolden an adversary during a nuclear standoff. Such attacks would pose serious escalation risks. Any state that fears its nuclear forces are at risk to cyber attacks might have incentives to use them early in a crisis because waiting could put it at a grave disadvantage. Knowing this, third parties looking to incite escalation between opponents could then spoof one adversary's NC3 during a crisis to make it appear as though it is under attack by the other. Last, some NC3 capabilities are reportedly dependent on dual-use platforms such as sensory and communications satellites. Cyber attacks on those systems could unintentionally appear as an attack on the other's strategic deterrent.

These types of concerns are already being discussed and addressed among countering-WMD experts within the U.S. nuclear enterprise. It is also a topic that receives considerable attention among nuclear specialists in the academic and think tank communities.[11]

Cyber as a WMD-Enabler and Amplifier

Cyber operations are increasingly prevalent in modern warfare. Cyber weapons can be used to better enable kinetic attacks by disabling or manipulating sensors or first-line security systems, communications, and response-targeting capabilities. Adversaries could use cyber in similar ways to facilitate WMD attacks on defended targets or hinder U.S. (local, state, and Federal) emergency response capabilities in ways that magnify the consequences of an attack. For instance, a cyber attack on the security system at a sensitive facility might allow an attacker to enter undetected in order to release a chemical or biological agent. Spoofing attacks on U.S. sensing and/or first responder communications might then frustrate U.S. capabilities to mitigate the effects and disabling cyber attacks on the healthcare infrastructure could impede any subsequent medical response. Similarly, an adversary might engage in a public disinformation cyber campaign in the aftermath of an attack to sow confusion and distrust in ways that compound the consequences.

Cyber as a Counterproliferation Tool

Cyber weapons can also disable or disrupt adversary WMD programs that depend on cyber technologies. The widely reported 2010 Stuxnet attack on an Iranian uranium enrichment facility is a case in point. Experts suggest that Stuxnet was a form of malware designed to spread across the globe from one computer to the next but to unleash its payload only when it entered an industrial control system with the characteristics of Iran's uranium enrichment facility at Natanz.[12] Once inside, it reportedly altered the system's program to monitor and regulate the supersonic spin of centrifuges in a way that led them to become unstable and ultimately breakdown. The attack demonstrated the ability of cyber weapons to penetrate and hobble adversary development of WMD.

Conclusion

In sum, the WMD Center does not consider cyber weapons to be WMD because they currently lack the proven potential for lethal effects that are comparable to CBRN, there are no international legal considerations equivalent to those surrounding WMD, and because of the contrast between cyber and WMD in terms of their mechanisms, historical employment, perceived utility, and proliferation challenges.

On a practical level, the technical knowledge pertaining to (countering) CBRN and cyber threats is substantially different, requiring distinct and dedicated expertise, bureaucratic structures, and operational authorities.

The growing connections between cyber weapons and WMD, however, justify close monitoring and sustained engagement from the community tasked with preventing and countering WMD threats. At a minimum, attention should be given to breaking down bureaucratic silos and facilitating greater dialogue between the cyber and countering-WMD communities to ensure U.S. policies and capabilities stay ahead of the evolving threat. In the future, the meaning of WMD and the U.S. approach to addressing related threats may need to be reconsidered, as the scale and scope of cyber threats grow.

Notes

1 James Garamone, "Vice Chairman Discusses Weapons of Mass Destruction at Symposium," *Defense News*, September 17, 2020, available at <https://www.defense.gov/Explore/News/Article/Article/2351492/vice-chairman-discusses-weapons-of-mass-destruction-at-symposium/>.
2 W. Seth Carus, *Defining "Weapons of Mass Destruction:" Revised and Updated*, Center for the Study of Weapons of Mass Destruction Occasional Paper, No. 8 (Washington, DC: NDU Press, 2012).
3 Melissa Eddy and Nicole Perlroth, "Cyber Attack Suspected in German Woman's Death," *New York Times*, September 18, 2020.
4 John P. Caves, Jr., and W. Seth Carus, *The Future of Weapons of Mass Destruction: An Update*, National Intelligence University Presidential Scholar's Paper (Washington, DC: National Intelligence Press, February 2021).
5 United Nations Conference on Disarmament, Prohibition of the Development and Manufacture of New Types of Weapons of Mass Destruction and New Systems of Such Weapon (New York: United Nations, January 7, 1997).
6 Releasing dangerous biological pathogens into the environment through cyber means is less likely; institutions working with them typically do not possess them in bulk, and they are not processed in quantity in cyber-enabled systems. A more likely threat would be cyber intrusions that facilitate an insider at such a facility obtaining access to an agent he or she would not ordinarily have access to.
7 President's National Infrastructure Advisory Council (NIAC), *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure* (Washington, DC: NIAC, August 2017, available at <https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>.
8 Nuclear Posture Review (Washington, DC: Department of Defense, February 2018), available at <https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF>.
9 Alexandra Van Dine, Michael Assante, and Page Stoutland, *Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities* (Washington, DC: Nuclear Threat Initiative, December 2016), available at <https://www.nti.org/analysis/articles/outpacing-cyber-threats-priorities-cyber-security-nuclear-facilities-paper/>; U.S. Government Accountability Office (GAO), *Critical Infrastructure Protection: Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities* (Washington, DC: GAO, May 2020), available at <https://www.gao.gov/assets/gao-20-453.pdf>.
10 Defense Science Board, *Task Force on Cyber Deterrence* (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, February 2017), available at <https://apps.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf>; Page O. Stoutland and Samantha Pitts-Kiefer, *Nuclear Weapons in the New Cyber Age: Report of the Cyber-Nuclear Weapons Study Group* (Washington, DC: Nuclear Threat Initiative, September 2018), available at <https://media.nti.org/documents/Cyber_report_finalsmall.pdf>.
11 See, for instance, information about a Cyber-Nuclear Weapons Study Group at the nongovernmental Nuclear Threat Initiative Web site, available at <https://www.nti.org/about/projects/cyber-nuclear-weapons-study-group/>; Aerial E. Levite et al., *China-U.S. Cyber-Nuclear C3 Stability* (Washington, DC: Carnegie Endowment for International Peace, 2021).
12 Dorothy E. Denning, "Stuxnet: What Has Changed?" *Future Internet*, No. 4 (July 2012), 672–687.

The mission of the Center for the Study of Weapons of Mass Destruction is to prepare U.S. national security leaders to address the challenges posed by weapons of mass destruction through its education, research, and outreach programs.

CENTER FOR THE STUDY OF WEAPONS OF MASS DESTRUCTION

Mr. Brendan Melley
Director

The Proceedings series presents key discussions, ideas, and conclusions from National Defense University symposia, workshops, strategic exercises and other research, and occasionally those of international counterparts. The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other agency of the Federal Government. For information on NDU Press, visit www.ndu.edu/press.

NDU Press