Innovation in Countering Weapons of Mass Destruction

- Arms Control Today

July/August 2015

By Andy Weber and Christine L. Parthemore

In April, Secretary of Defense Ash Carter traveled to Silicon Valley to meet with technology industry leaders and signal his intent to lead the Department of Defense in the direction of greater innovation. Although his visit focused heavily on cybersecurity, it is critical to apply his vision to the task of preventing and preparing for crises involving weapons of mass destruction (WMD). As these threats can evolve quickly, testing the United States' ability to adapt, a broad understanding of how to apply technological solutions is crucial.

Investments by the U.S. government and its international partners often focus too narrowly on invention of entirely new tools and systems. In many cases, governments do not need to invent new, "game-changing" technologies in order for technology to change the game. Effectively countering WMD threats requires not just invention, but true innovation as Carter described it, including applying existing technologies in new ways, changing processes to gain efficiencies, and finding creative applications for tools that are already available.

There are many cases in which rapid and creative use of existing and often low-tech capabilities is the fastest option for altering the trajectory of nuclear, biological, and chemical weapons threats. The challenge of destroying the declared stockpile of Syrian chemical weapons proved that one of the best ways to address modern WMD threats can be simply to help an organization to rapidly use existing technologies in new ways.

This article will explore such an approach to countering WMD threats and describe how focusing more attention on innovation, especially by taking advantage of existing technologies in novel ways to rapidly prevent proliferation or use of nonconventional weapons and dual-use technologies, would be cost effective and improve the ability of the United States and other countries to respond with speed as threats evolve. Furthermore, this approach is crucial to democratizing the process of countering proliferation threats by ensuring that lower-income countries can contribute to efforts to counter WMD threats and by expanding opportunities for the private sector and individual citizens to help mitigate nuclear, biological, and chemical weapons dangers.

The Element of Time

It often seems that WMD threats are relics of past eras—ancient methods kept alive as the character of warfare modernizes. The world recently marked the 100th anniversary of modern battlefield use of chemical weapons. Use of biological means to defeat or subjugate adversaries goes back hundreds of years, possibly to ancient times. Nuclear threats are frequently described as a threat of the Cold War era more than a current challenge.

In fact, the threats from these nonconventional weapons pose some of the greatest contemporary security challenges, in part because they are often characterized by rapid evolution and a tendency to increase in urgency with little warning time.

The United States and its partners have many important baseline tools to counter WMD threats. Treaty negotiations, export control systems, arms control efforts, and long-term research and

development initiatives form an important foundation for preventing proliferation and use of nonconventional weapons. Yet, the ability to act quickly as new threats emerge—often in weeks or months, not years—is critical but underappreciated. Innovation is often the best path to success.

Success With Syrian Chemicals

The Defense Department's contribution to the destruction of Syria's chemical weapons stands as a textbook example of the role rapid innovation can play in mitigating WMD threats. The stockpile of chemical weapons materials that Syrian President Bashar al-Assad declared to the international community in his quest for regime survival included mustard agent, ingredients to formulate sarin and VX agents, and smaller quantities of other substances used in the country's chemical weapons program. The Assad regime stored most of the chemicals in bulk liquid form in hundreds of barrels and tanks rather than filled weapons that were ready for use. The chemicals were dispersed at sites around the country as it descended into a protracted and brutal civil war.

In late 2012, Pentagon scientists and engineers were asked to envision how any country, given the opportunity, would go about destroying chemicals like those then held by the Assad regime. Many chemical weapons ingredients can be destroyed in incinerators, but others are better or more quickly destroyed using an initial hydrolysis process to alter the chemicals into substances that incinerators can more easily handle without damage. The most dangerous 600 metric tons of Syria's 1,300 metric tons of chemical weapons materials fell into the latter category.

Most facilities that conduct chemical weapons destruction operations are large, expensive, and built for a specific location. Removing Syria's chemicals to one of these facilities most likely would have been impossible in the face of international legal questions and political and logistical constraints. Yet, no country in the world had an easily transportable technology that could rapidly destroy large quantities of bulk liquid chemical weapons materials. With no desire by the United States or others to construct a fixed facility in the middle of Syria's civil war, the Defense Department's top WMD destruction experts were formally tasked in January 2013 with developing a hydrolysis system that could be transported to any location in the world where destruction operations could be conducted safely.

Within six months, the first unit stood in a containment tent in the summer sun at Aberdeen Proving Ground in Maryland. Looking at the Field Deployable Hydrolysis System (FDHS), as its creators named it, one sees a maze of pipes, pumps, tanks, and hoses fixed within two standard shipping containers. When fully assembled on land, several additional shipping containers were arrayed around the FDHS to heat water, analyze the chemicals that are pumped through the system, and perform other standard support functions. Through the summer of 2013, it was not known where or when the systems, which could be assembled for use within 10 days, might be used. The Defense Department requested that seven units be developed in order to maximize its options. For example, the department was able to consider sending a few of the seven units to locations in or near the Middle East to be quickly assembled in case the Assad regime's loss of territory led to small batches of dangerous chemicals becoming available for the international community to destroy.

In order to have equipment available within six months, department experts drew on the technical knowledge they already had, modified commercially purchased items, and used some equipment already in the Pentagon's inventory. With extensive chemical weapons demilitarization experience informing their work, the department's engineers, chemists, and managers adapted proven chemical neutralization capabilities to rapidly develop a novel solution.

The FDHS solution was elegant and straightforward. Perhaps more importantly, it was developed quickly enough to influence an increasingly urgent challenge. It made it possible for the United States to convince the world that physical removal of chemical materials for destruction outside Syria was feasible and desirable. Innovation quickly created new options for successfully countering one of the world's most pressing WMD threats.

On Ebola, Mixed Results

The 2014–2015 outbreak of the Ebola virus in West Africa is a stark case of the need for rapid response to unpredictable threats as they emerge. Countless existing tools could have helped in the Ebola response if the United States and other states assisting the affected countries had used them more rapidly. Although the effort to stop Ebola included some successes, responders could have better applied information technologies, diagnostics, and other tools.

One factor that worked in favor of the response effort was that, for years, the Defense Department biodefense program and its partners in other U.S. agencies had been developing capabilities to prevent, detect, and respond to dangerous infectious diseases, including the Ebola virus. Rapid deployment of U.S. Navy and Army mobile diagnostic laboratories to Liberia had a huge impact on curbing the epidemic last fall. In key affected areas, the time to diagnosis, which had been five to seven days, was reduced to three to five hours. This dramatically reduced the burden on Ebola treatment units—the specialized spaces set up to diagnose and treat Ebola patients—and those showing symptoms in ways that minimized potential exposure of others to the virus.

Lack of innovation on the information technology and biosurveillance front, however, impeded an effective response. Although the Pentagon had developed a suite of advanced biosurveillance systems through activities such as the Able Response bioterrorism exercise series with South Korea, bureaucratic hurdles hampered the U.S. government’s ability to share them with West African governments, international nongovernmental organizations, and other key players on the ground. Now that the scale of the Ebola crisis has waned, private partners such as the Paul G. Allen Family Foundation, Facebook, and NetHope are fostering data system innovation to prepare for future pandemics, but such tools were not applied rapidly enough to meet their full potential in countering Ebola’s spread.

Leveraging Existing Technology

Given these lessons from recent experiences in two critical efforts, it is timely to consider how nuclear, chemical, and biological weapons threats can be mitigated in novel ways by government agencies leveraging commercial technologies more effectively and creatively. In the future, information technology tools and methods commonly available in the private sector are likely to play a more central role in preventing proliferation, enhancing verification capacity, revolutionizing information sharing, and facilitating rapid decision-making in case of a chemical, biological, or nuclear attack. For example, positive inventory control systems commonly used in the private sector could be applied to improving the security and real-time accounting of nuclear, biological, and chemical materials. The Defense Department is adapting “smart freezers” that know and report the details any time they are opened and biological materials are entered or removed.

Monitoring, tracking, and surveillance could likewise be improved by applying current technologies more effectively. A huge opportunity exists for the United States and other countries to adapt commercial tracking and monitoring systems in the battle to secure nuclear materials. Many analysts are developing concepts to use societal verification that include the public use of ubiquitous technologies to identify potential WMD threats and reduce proliferation possibilities. Mobile telephone videos posted on Twitter and YouTube played a key role in identifying and documenting the Syrian regime’s hideous attack of August 13, 2013, which killed approximately 1,400 innocent men, women, and children.

Other opportunities lie in finding unique ways to enhance the connectivity of existing data repositories and reporting systems in order to boost the world’s ability to prevent and respond to biological and global health threats. The private sector is rapidly advancing new tools and techniques in diagnostics, bringing down costs, decreasing response times, and minimizing the need for diffuse laboratories to hold samples of dangerous pathogens by reducing the need to develop cultures. Great advances in reducing biological risks can be made through better and more creative application of these private-sector advances—a challenge facing the U.S. government broadly.

The security imperative of effectively reducing WMD threats justifies a renewed focus on innovating with existing technologies and tools. This approach carries secondary benefits as well. It is responsive to budget constraints and can help show countries that countering the proliferation and use of nuclear, biological, and chemical weapons materials does not always require billions of dollars.

The U.S. executive branch has operated within mounting budget pressures for several years and can reasonably assume this condition will continue. The FDHS units cost a few million dollars each—extremely affordable by Pentagon standards and well within a range the department’s leaders

were willing to provide in order to expand the list of available options for addressing the Syrian chemical weapons threat. With the FDHS experience as a guide, government agencies should experiment more with ideas for promoting innovation in countering nonconventional weapons through open, public challenges and X Prize-style competitions. The Defense Department has used such contests in energy and robotics to find rapid and effective solutions that are far more affordable than traditional, long-term research and development initiatives. These models should be embraced for diagnostic, characterization, surveillance, tracking, and other types of tools that aid in reducing WMD threats.

To truly ensure that the United States can find effective and affordable pathways for countering WMD threats in the future, the country's leaders must convey that addressing nuclear, chemical, and biological weapons challenges is a shared mission to be met collectively by all like-minded countries. Technology can play a crucial role in this narrative. Yet, too frequently, high-income countries promote programs to mitigate biological, chemical, and nuclear weapons threats that rely on tools and methods with unsustainably high life-cycle costs.

U.S. partnerships to thwart proliferators could include projects that focus on innovation that helps achieve jointly desired outcomes rather than relying on set road maps dictating multiyear research plans. Finding new ways to apply low-tech solutions to evolving threats can also show partner countries that the United States is committed to creative collaboration to address WMD challenges and that Washington is not interested solely in selling expensive U.S. technologies. No matter what the approach, there are many ways to democratize countering WMD threats by ensuring that lower- and middle-income countries without funds to expend on new inventions and breakthroughs can still creatively contribute.

Finally, government agencies must find effective ways to leverage the best work being advanced by academic and private-sector enterprises and to expand opportunities for small companies and individual citizens to help mitigate nuclear, biological, and chemical weapons threats. This challenge transcends the counter-WMD enterprise, to be sure. As the Defense Department works to improve acquisition processes and make government contracts attractive to all companies—not just those that best know government contracting processes—it should keep in mind that its good work can open doors for effectively reducing truly catastrophic nuclear, chemical, and biological weapons threats.

Conclusion

In his Stanford speech, Carter stated, "I don't want us to lose out on an innovative idea or capability we need because the Pentagon bureaucracy was too slow to fund something, or we weren't amenable to working with startups, as we should be."[1] This is a critical point for a Defense Department grappling with questions of how to operate in a new era of constant change. WMD threats will continue to evolve, testing the U.S. ability to adapt. Those charged with countering these threats must embrace an approach that includes robust support for true innovation.

Andy Weber served as assistant secretary of defense for nuclear, chemical, and biological defense programs until October 2014 and then as deputy Ebola coordinator at the Department of State until he retired from the U.S. government in May. **Christine L. Parthemore** was a senior adviser in the nuclear, chemical, and biological defense programs office and is now affiliated with Johns Hopkins University and the Center for American Progress.

ENDNOTE

1. Ash Carter, "Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity" (speech, Stanford University, April 23, 2015), http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1935.