Preventing Weapons of Mass Destruction Proliferation– Leveraging Special Operations Forces to Shape the Environment

by

Colonel Lonnie Carlson, Ph.D., and Margaret E. Kosal, Ph.D.

Joint Special Operations University

Center for Special Operations Studies and Research

JSOU Press

Occasional Paper

January 2017

On the cover: U.S. Army Sgt. 1st Class Matthew Carpenter, assigned to U.S. Army Special Operations Command, conducts chemical, biological, radiological, and nuclear decontamination during the 2014 U.S. Army Best Warrior Competition. Source: U.S. Army photo by Staff Sgt. Patricia Ramirez.

Note: This paper was originally written as a U.S. Army War College research paper.

About the Authors

Colonel Lonnie Carlson, Ph.D.
U.S. Army

Colonel Lonnie Carlson is a U.S. Army nuclear and counterproliferation officer [Functional Area 52]. He advises senior leadership in strategic and operational level civilian and military organizations on strategy, policy, plans, and programs to counter adversary weapons of mass destruction (WMD) programs, as well as efforts to sustain and modernize the U.S. strategic deterrent. He previously worked on countering WMD strategy, policy, plans, and programs at U.S. European Command (USEUCOM), and nuclear weapon and infrastructure capabilities and resources at U.S. Strategic Command (USSTRATCOM).

Colonel Carlson received a Ph.D. in materials engineering from the University of Nebraska–Lincoln, an M.S. in nuclear engineering from the Air Force Institute of Technology, and a B.S. in aerospace engineering from the University of Colorado–Boulder. He entered the U.S. Army Reserves as an infantryman in 1987, and received a commission in the active Army as an air defense officer in 1993 after attending the University of Colorado on an ROTC scholarship.

Margaret E. Kosal, Ph.D.
Associate Professor, Sam Nunn School of International Affairs, Georgia Institute of Technology, and Director, Sam Nunn Security Program

Dr. Margaret E. Kosal is an associate professor in the Sam Nunn School of International Affairs at the Georgia Institute of Technology and director of the Sam Nunn Security Program. For the 2016–2017 academic year, she has been appointed Senior Adjunct Scholar to the Modern War Institute at West Point. Her research explores the relationships among technology, strategy, and governance. She focuses on two, often intersecting, areas: reducing the threat of WMD and understanding the geopolitics of emerging technologies. She is the author of *Nanotechnology for Chemical and Biological Defense*, which explores scenarios, benefits, and potential proliferation threats of nanotechnology and other emerging sciences.

Formally trained as an experimental scientist, she earned a doctoral degree in chemistry from the University of Illinois at Urbana-Champaign working on biomimetic and nano-structured functional materials. She is co-founder of a sensor company, where she led research on medical, biological, chemical, and explosive detection. Dr. Kosal previously served as senior advisor to the chief of staff of the U.S. Army, as science and technology advisor within the Office of the Secretary of Defense, and as an associate to the National Intelligence Council, among other consulting. She is the recipient of multiple awards, including the Office of the Secretary of Defense Award for Excellence, and recently was appointed the next editor-in-chief of the Cambridge University Press journal, *Politics and the Life Sciences*.

Preventing Weapons of Mass Destruction Proliferation–
Leveraging Special Operations Forces to Shape the Environment

The greatest danger of another catastrophic attack in the United States will materialize if the world's most dangerous terrorists acquire the world's most dangerous weapons.

—The 9/11 Commission Report[1]

In 1998, the leader of the al-Qaeda terrorist group, Osama bin-Laden, stated that acquiring weapons of mass destruction (WMD) to defend Muslims was a religious duty.[2] To further clarify their position, al-Qaeda released a statement in 2002 saying they felt justified to "use WMD to kill four million Americans."[3] It is highly unlikely the al-Qaeda desire for WMD died with bin-Laden in 2011. The current al-Qaeda leader, an Egyptian surgeon named Ayman al-Zawahiri, personally led al-Qaeda's strategic nuclear and biological acquisition programs prior to bin-Laden's death.[4] These were not makeshift, amateur programs. Al-Zawahiri focused on recruiting highly educated scientists and running multiple, separately compartmented bioweapon development programs.[5] Al-Qaeda simultaneously scoured the globe seeking to purchase nuclear weapons or the nuclear fuel to create their own.[6] Despite significant disruption to al-Qaeda operations, their strategic patience and long view remain concerning.

Daesh (a.k.a. Islamic State in Iraq and Syria [ISIS] or Islamic State in Iraq and the Levant [ISIL]) has not been as overt as al-Qaeda in stating their desire to acquire WMD, but they appear to be actively seeking the opportunity, even if not as organized and strategically oriented as al-Qaeda. In 2015, Daesh sought to buy alleged nuclear materials in Moldova and used captured chemicals as weapons in Iraq and Syria.[7] There should be little doubt Daesh would use even more catastrophic weapons if they acquire them.

---

[1] Thomas H. Kean and Hamilton Lee, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. (Washington, D.C.: National Commission on Terrorist Attacks Upon the United States, 2004), 380, accessed 8 February 2016 at: http://www.9-11commission.gov/report/911Report.pdf.
[2] Rolf Mowatt-Larssen, "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" Paper, Belfer Center for Science and International Affairs, Harvard University, January 2010, 13, accessed 8 February 2016 at: http://belfercenter.ksg.harvard.edu/publication/19852/al_qaeda_weapons_of_mass_destruction_threat.html.
[3] Ibid., 23.
[4] Ibid., 12.
[5] Ibid., 12, 14–16, 19, 22–23.
[6] Ibid., 12, 15, 21, 26.
[7] Desmond Butler and Vadim Ghirda, "Nuclear smugglers tried selling materials to ISIL," Associated Press, 7 October 2015, accessed 8 February 2016 at: http://www.usatoday.com/story/news/world/2015/10/07/ap-nuclear-smugglers-tried-selling-materials-isil/73501960/; and James. R. Clapper, Director of National Intelligence, "Opening Statement,

Multiple U.S. national strategies state that countering the proliferation and use of WMD is among the highest national priorities and requires a whole of government effort.[8] Countering WMD proliferation is not a simple task, however, as proliferation involves a broad range of actors, materials, technologies, activities, and legal considerations that affect the roles of military and civilian government departments. Considerations such as risk, time sensitivity, geographic location, and international relations further complicate the situation. Despite the challenges of countering WMD (CWMD), the U.S. Government (USG) must dedicate the necessary resources to defeat the clear desire of terrorist groups to obtain and use WMD in mass casualty attacks against U.S. citizens and our allies.[9]

In order to provide guidance to organizations within the Department of Defense (DOD), the Secretary of Defense issued a new DOD Strategy to Counter Weapons of Mass Destruction in June 2014 with a "focus on cooperative efforts to shape the security environment and take early action against adversaries."[10] In support of national and DOD CWMD strategies, U.S. Special Operations Command (USSOCOM) seeks to understand how Special Operations Forces (SOF) can better support WMD counterproliferation efforts and what the appropriate balance between WMD risks is.[11]

The CWMD mission area is so broad it is necessary to limit the scope of this paper to leveraging SOF to counter the proliferation of illicitly trafficked weapons, materials, and supporting equipment and knowledge. For a broader view of the DOD challenge in CWMD, particularly WMD elimination, see efforts such as U.S. Army CWMD strategic studies.[12]

Understanding the options for how SOF can better support WMD counterproliferation efforts first requires the answers to three questions:

- What are the primary risks and threats to U.S. interests from WMD proliferation?
- What are the key elements to disrupting or defeating a proliferation network?
- What unique capabilities can SOF provide?

Senate Armed Services Committee Hearing—IC's Worldwide Threat Assessment," 9 February 2016, accessed 18 February 2016 at: http://www.dni.gov/files/documents/2016-02-09SASC_open_threat_hearing_transcript.pdf .

[8] U.S. National Security Council, *Strategy to Combat Transnational Organized Crime* (Washington, D.C.: U.S. National Security Council, July 2011), 14; White House Office, *National Strategy for Counterterrorism* (Washington, D.C.: White House Office, June 2011), 8; U.S. National Security Council, *National Strategy for Countering Biological Threats* (Washington, D.C.: U.S. National Security Council , November 2009), 2; and U.S. Joint Chiefs of Staff, *National Strategy to Combat Weapons of Mass Destruction* (Washington, D.C.: U.S. Office of the Chairman of the Joint Chiefs of Staff, December 2002), 1.

[9] Brad Roberts, "Deterrence and WMD Terrorism: Calibrating Its Potential Contributions to Risk Reduction," Paper, Institute for Defense Analyses, June 2007, 5, accessed 8 February 2016 at: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA470305.

[10] U.S. Department of Defense, *Department of Defense Strategy to Counter Weapons of Mass Destruction (WMD)*, (Washington, D.C.: U.S. Department of Defense, June 2014), v.

[11] Robert Nalepa, ed., Special Operations Research Topics 2016, (Tampa, FL: Joint Special Operations University, 2015), 39, accessed 8 February 2016 at: https://jsou.socom.mil/JSOU%20Publications/2016_SpecialOperations ResearchTopics_final.pdf.

[12] Chief of Staff of the Army Strategic Studies Group I, Design and Employ the Force End of Program Report, (Washington, D.C.: U.S. Army, June 2013).

This paper argues that the critical shortfall in preventing WMD proliferation is a lack of detailed understanding of proliferation networks by U.S. and partner security forces. This failure to understand the environment leads to a lack of timely indications, warning, and actionable intelligence needed to conduct time-sensitive operations against fleeting WMD proliferation targets. To mitigate this shortfall, USSOCOM must build WMD expertise within SOF, and collaborate with USG and partner nation organizations to conduct WMD counterproliferation-related building partnership capacity (BPC) and operational preparation of the environment (OPE) activities.

SOF Attributes

The 'SOF Truths'[13] capture both the creativity and flexibility SOF are known for, but also their limited ability to quickly grow capacity and operate long-term without support of other partners. These attributes inform the development of SOF theory.

The 'SOF Truths' highlight both the strengths and limitations of SOF. Source: *U.S. Special Operations Command Fact Book*

The first attempts to define special operations theory by William H. McRaven (who later became commander of USSOCOM), James D. Kiras, and Robert G. Spulak focused on the tactical and strategic elements of 'direct action' combat operations.[14] It was William Harris, though, who defined the principle of SOF conducting irregular warfare (IW) by, with, and through partners.[15]

Harris defines IW as strategic competition against irregular threats in the domain of weak government institutions.[16] The IW characteristics Harris defines extend beyond typical irregular threats such as guerilla war or subversion into WMD counterproliferation. The difficulty in IW of projecting power over distance,

[13] USSOCOM Public Affairs, *SOF Truths*, http://www.socom.mil/Pages/SOFTruths.aspx.
[14] William H. McRaven, The Theory of Special Operations, Thesis, (Monterey, CA: U.S. Naval Postgraduate School, June 1993), 5; James D. Kiras, *Special Operations and Strategy: From World War II to the War on Terror* (New York: Routledge, 2006), 4; and Robert G. Spulak, *A Theory of Special Operations* (Hurlburt Field, FL: Joint Special Operations University Press, 2007), 1.
[15] William D. Harris, Jr., *Special Operations, Irregular Warfare, and Operational Art: A Theory of Special Operations*, Monograph (Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, October 2013), 18; Colin S. Gray, "Handfuls of Heroes on Desperate Ventures: When Do Special Operations Succeed?" *Parameters*, Spring (1999): 2–24; and Linda Robinson, *Masters of Chaos: The Secret History of the Special Forces* (New York, NY: Public Affairs, 2004).
[16] Harris, *Special Operations, Irregular Warfare, and Operational Art*, 16.

achieving strategic effect through tactical action, and coalition building are equally applicable to CWMD activities.[17] Harris further defines tenets of SOF IW operational art that can extend to WMD counterproliferation campaigns. Particularly relevant are those of cognitive and physical access needed to gain access to, and develop an understanding of, the operational area.[18]

As SOF have developed significant direct action expertise since 11 September 2001 (9/11), it is in the IW domain that SOF have the greatest opportunity to significantly improve U.S. WMD counterproliferation effectiveness.

WMD Risks

This paper limits the definition of WMD to chemical, biological, radiological, and nuclear (CBRN) weapons. Assessments of the risk of WMD use vary greatly within policy and academic communities, largely due to the difficulty in quantifying the probability of acquisition of weapon quality materials by state and non-state actors.[19] This difficulty results in USG policy and strategy documents generally lacking specific priorities needed to effectively allocate CWMD resources. The common theme is to state that the greatest time-sensitive risk to U.S. interests is WMD, particularly nuclear and biological weapons, in the hands of terrorists.[20] Less time-sensitive, but still articulated as strategically important, is proliferation of WMD program technology to potentially malign state actors such as Iran.[21] Outside of department-level acquisition requirements documents, specific radiological and chemical weapon counterproliferation priorities are largely absent in publicly available USG national strategy documents.

The wide range of CBRN materials and weapons also constitutes a wide range of strategic risks. Understanding the level of risk in terms of potential costs and probability of use helps quantify the level of concern and time sensitivity associated with each type and defines the relative roles of SOF and law enforcement.

Nuclear Weapons

USG policy documents clearly state that the highest consequence WMD risk in terms of potential loss of life, financial cost, and impact on global stability is nuclear weapon use by terrorists or malign states.[22] Time-sensitive nuclear threats by terrorists or adversary states are broken into two categories: the impending acquisition and use of nuclear weapons, and the proliferation of fissile

[17] Ibid., 35.
[18] Ibid., 38.
[19] Gregory D. Koblentz, "Predicting Peril or the Peril of Prediction? Assessing the Risk of CBRN Terrorism," *Terrorism and Political Violence* 23, no. 4 (2011): 502.
[20] National Security Council, *National Security Strategy* (Washington: D.C.: National Security Council, February 2015), 11.
[21] Ibid.
[22] Ibid.

nuclear materials of concern, such as uranium-235 and plutonium-239, that are needed to develop nuclear weapons.[23]

Experts disagree on the exact probability that terrorists will acquire either a nuclear weapon or sufficient nuclear materials for a weapon, but there is general agreement that the probability is relatively low.[24] To date, there have been no known attempts to sell nuclear weapons, but the USG and partners seized small quantities of nuclear materials of concern for sale on the black market.[25] Based on the extreme consequences of failure, USG policy is that preventing proliferation of a lost or stolen nuclear weapon anywhere in the world is the highest, most time-sensitive national priority and includes a prominent role for SOF.[26] As the development of improvised nuclear weapons is not particularly challenging, the proliferation of weapon-sufficient quantities of nuclear materials, such as weapons-grade uranium and plutonium, is also a time-sensitive priority suitable for SOF employment.

Due to the high security of U.S. nuclear weapons and materials, nuclear weapon or nuclear materials threats are most likely to originate outside the U.S. and proliferate through existing illicit trafficking networks. As there are 24 known or suspected states with nuclear weapons and weapons-grade nuclear materials (see Table 1), tracking the proliferation of nuclear materials out of these states into transit zones is "relatively" easier than CBR materials with essentially worldwide availability.

Argentina	France*	Japan	Poland
Australia	Germany	Kazakhstan	Russia*
Belarus	India*	Netherlands	South Africa
Belgium	Iran	North Korea*	Switzerland
Canada	Israel*	Norway	United Kingdom*
China*	Italy	Pakistan*	United States*

Table 1. States with weapons-usable nuclear materials. States marked with an * are known or suspected to possess nuclear weapons.[27]

A less immediate risk is the development, or continued development, of nuclear weapon programs by adversarial states such as Iran and North Korea. Although it is disconcerting that states seek nuclear weapons and a potential electromagnetic pulse (EMP) capability, there is less expectation that they will actually use them compared to an ideologically driven terrorist group due to more traditional state-state deterrence mechanisms.[28] The EMP concern from non-state

[23] International Atomic Energy Agency, *Combating Illicit Trafficking in Nuclear and Other Radioactive Material: Technical Guidance, Reference Manual* (Vienna: International Atomic Energy Agency, 2007), 3, accessed 8 February 2016 at: http://www-pub.iaea.org/MTCD/publications/PDF/pub1309_web.pdf.
[24] Koblentz, "Predicting Peril or the Peril of Prediction?," 502.
[25] Butler and Ghirda, "Nuclear smugglers tried selling materials to ISIL."
[26] National Security Council, *National Security Strategy*, 11.
[27] Nuclear Threat Initiative, *The 2016 NTI Nuclear Security Index: Theft and Sabotage: Building a Framework for Assurance, Accountability, and Action*, 3rd Edition (Washington, D.C.: Nuclear Threat Initiative, January 2016), 20, accessed 8 February 2016 at: http://www.ntiindex.org.
[28] Roberts, "Deterrence and WMD Terrorism," 26.

actors is minimal due to their inability to detonate a nuclear weapon in the exoatmosphere, where EMP can cause significant widespread damage, unlike surface or low-atmospheric detonations that produce significantly reduced EMP effects. Although preventing this type of technology proliferation is generally more law enforcement–centric, there is still an opportunity for SOF network analysis and disruption capabilities supported by regional persistent presence to facilitate U.S. and DOD counterproliferation efforts.

Radiological Weapons

Radiological weapons do not receive particular emphasis in national-level strategy documents but are characterized in key departmental-level documents.[29] Radiological weapons differ from nuclear weapons in that they do not create a yield-producing explosion or EMP, but instead expose people and infrastructure to radioactive contamination. Despite doing little direct damage beyond that of the explosion, if a simple radiological dispersal device (RDD) exploded in a major city or sea/airport, it would likely result in billions of dollars of cleanup costs and a new round of expensive security and detection upgrades. Because radiological material thefts from medical and industrial facilities are common worldwide, the probability of use is relatively higher than of nuclear weapons while the consequence is lower.[30] This relatively easy access reduces incentives for a terrorist organization to try to smuggle radiological materials into the U.S. versus stealing them locally.

Conventional terrorist attacks against nuclear power plants are a well-considered problem that has resulted in significant security upgrades, particularly since 9/11.[31] What is increasingly of concern, however, are cyber attacks against nuclear power plants and storage facilities. A recent survey of legal requirements to protect these facilities against cyber attacks indicates many nuclear power nations have no requirements to protect or exercise against cyber attack.[32] Within the U.S. homeland, the protection of radiological materials and nuclear facilities belongs to private industry and law enforcement agencies. Overseas, there may be a role for SOF to collaborate with U.S. and partner nation security forces depending on the potential risk of radiological weapons in the host nation.

Biological Weapons

Similar to nuclear weapons, national policy documents routinely address biological weapon threats, but do little to articulate threat priorities relative to other types of WMD.[33] Biological

[29] National Nuclear Security Administration, *Prevent, Counter, and Respond—A Strategic Plan to Reduce Global Nuclear Threats (FY 2016–FY 2020)*, Report to Congress (Washington, D.C.: National Nuclear Security Administration, March 2015), 3-1, available at: https://nnsa.energy.gov/sites/default/files/NPCR%20Report_FINAL_4-14-15.pdf.
[30] Center for Nonproliferation Studies, *CNS Global Incidents and Trafficking Database, 2014 Annual Report*, April 2015, 6, accessed 12 March 2016 at: http://www.nti.org/analysis/reports/cns-global-incidents-and-trafficking-database/.
[31] International Atomic Energy Agency, *Combating Illicit Trafficking*, 4.
[32] Nuclear Threat Initiative, *The 2016 NTI Nuclear Security Index*, 4.
[33] U.S. National Security Council, *National Strategy to Counter Biological Threats*, 2.

weapon threats vary widely from highly transmissible and lethal diseases such as smallpox, to highly lethal but non-transmissible anthrax, to relatively low lethality and transmissibility agents such as salmonella. Although most biological weapons exist in nature or are sourced through illicit means, they are challenging to effectively weaponize without state-level resources, as demonstrated by the failed anthrax development attempts of the Aum Shinrikyo and al-Qaeda terror groups.[34] Preventing biological weapon proliferation is challenging due to the possibility of production in small facilities using common bioscience lab equipment. However, for successful weaponization, significant biology expertise is required.[35] Of concern is increasing potential for new biological weapon threats as tools used for DNA sequencing and genetic manipulation become faster and less costly.[36] The number of university biology labs with the tools needed to modify the genetic structure of viruses and bacteria and that can create new biological weapons resistant to treatment is growing rapidly due to low costs.[37] The maturing nexus between new nanotechnology and bioscience technologies also opens up entirely new options for biological weapons.[38]

Consensus is that biological weapons are the most likely WMD threat to the U.S., due to multiple previous anthrax, ricin, and botulism attacks with weapons created in the U.S.[39] While a significant challenge, these biological weapon threats have yet to cause more than a few casualties and are primarily domestic law enforcement and public health issues. Of greater relevance for SOF proliferation prevention efforts is the low probability but higher consequence use of weapons-grade biological material trafficked from illicit state or non-state actor biological weapon programs. A malign actor, whether terrorist or a state, does not have to create a highly effective or efficient weapon to stimulate a strong security and financial cost.

Chemical Weapons

Two types of chemical weapons concerns are military grade chemical weapons and toxic industrial chemicals/materials (TICs/TIMs). Countering the proliferation of chemical weapons is only broadly mentioned in national policy documents, but there is much more specific policy for

[34] Audrey Kurth Cronin, *Terrorist Motivations for Chemical and Biological Weapons Use: Placing the Threat in Context*, Report for Congress (Washington, D.C.: U.S. Library of Congress, Congressional Research Service, 28 March 2003), 5-6.
[35] U.S. Joint Chiefs of Staff, Joint Publication 3-40, *Countering Weapons of Mass Destruction*, 31 October 2014, II-10.
[36] Jerry Warner, James Ramsbotham, Ewelina Tunia, and James J. Valdes, "Analysis of the Threat of Genetically Modified Organisms for Biological Warfare," Center for Technology and National Security Policy, National Defense University, May 2011, 31, accessed 8 February 2016 at: http://ctnsp.dodlive.mil/files/2013/07/DTP-082.pdf.
[37] Mackenzie Foley, "Genetically Engineered Bioweapons: A New Breed of Weapons for Modern Warfare," *Dartmouth Undergraduate Journal of Science* XV, no. 2 (Winter 2013): 16.
[38] Margaret Kosal, *Nanotechnology for Chemical and Biological Defense* (New York, NY: Springer-Verlag, 2009), 91.
[39] Bob Graham, Jim Talent, et al., *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism* (New York, NY: Vintage Books, 2008), xv.

mitigating risks to U.S. chemical industry infrastructure.[40] A challenge with detecting chemical weapons proliferation, similar to biological weapons, is that many of the precursors and production tools are dual-use items with common industrial applications.[41] The use of chemical weapons by terrorists is considered a lower risk threat, despite being relatively easy to manufacture and having a higher probability of use, because they are challenging to effectively disperse and relatively easy to mitigate.[42] This is true of even industrial scale weapon programs such as that of Aum Shinrikyo in Japan, which had limited success during the Tokyo subway attacks.[43] Recent chlorine and mustard attacks by Daesh terrorists in Syria and Iraq highlight the will to use chemical weapons, but also demonstrate the challenge of creating mass effects without a rigorous development and weaponization program.[44]

Potentially of greater concern are terrorist attacks on industrial TIC/TIM sites near more populated areas causing significant casualties, particularly as cyber threats against infrastructure become increasingly common and sophisticated. There have been disrupted attacks on remote chemical storage sites that would have caused few casualties, but would require significant remediation cost.[45] The Department of Homeland Security and local governments recognize the industrial TIC/TIM threat and have developed critical infrastructure protection response plans in support of what is ostensibly a domestic law enforcement role.[46] Similar to radiological weapons, however, there is a plausible DOD role for prevention of chemical weapons proliferation overseas, in collaboration with U.S. law enforcement and partner nation security forces, if indications and warnings point to a significant risk.

Figure 1 conceptually captures the previous risk discussion.[47] The absence of a USG policy consensus on relative probability of use and potential costs is understandable due to the sheer number of material types and quantity combinations, making it challenging to assign specific levels of risk. Nonetheless, recent examples of chemical and biological weapon use and resulting effects, ongoing radiological material trafficking, and an understanding of nuclear and biological weapon consequences support the broad grouping of relative risks.

---

[40] U.S. Department of Homeland Security, *Chemical Sector–Specific Plan: An Annex to the National Infrastructure Protection Plan* (Washington, D.C.: U.S. Department of Homeland Security, 2010), 3.

[41] U.S. Joint Chiefs of Staff, Joint Publication 3-40, II-6.

[42] Barbara Stall, Jim Sciutto, and Elise Labott, "U.S. confirms ISIS used mustard agent," CNN, 14 August 2015, accessed 15 October 2015 at: http://www.cnn.com/2015/08/14/politics/isis-mustard-agent/index.html.

[43] Paul K. Kerr, *Nuclear, Biological, and Chemical Weapons and Missiles: Status and Trends*, Report for Congress (Washington, D.C.: U.S. Library of Congress, Congressional Research Service, 20 February 2008), 15–17.

[44] Morag MacKinnon, "ISIS is using chlorine as a weapon, Australia's Foreign Minister says," Reuters, 6 June 2015, accessed 8 February 2016 at: http://www.reuters.com/article/us-mideast-crisis-isis-chlorine-idUSKBN0OM05220150606; and Helene Cooper, "ISIS Is Suspected of a Chemical Attack Against Kurds in Syria," 14 August 2015, accessed 8 February 2016 at: http://www.nytimes.com/2015/08/15/world/middleeast/isis-suspected-of-chemical-attack-against-kurds-in-syria.html?_r=0.

[45] Alissa de Carbonnel and Steve Gutterman, "Russia says foils plot to attack chemical arms facility," Reuters, 15 October 2013, accessed 8 February 2016 at: http://uk.reuters.com/article/uk-russia-chemical-plot-idUKBRE99E06120131015.

[46] U.S. Department of Homeland Security, *Chemical Sector–Specific Plan*, 3.

[47] Author created figure based on analysis of references found in citations 20-47.

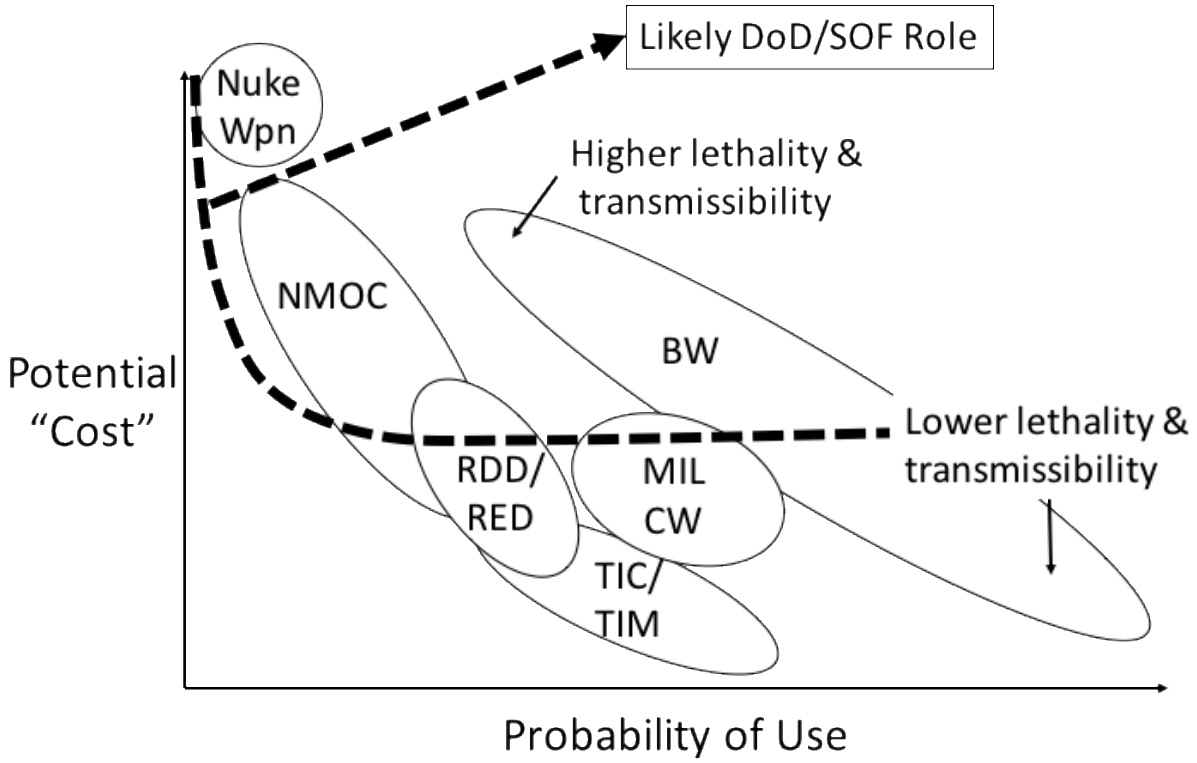


Figure 1. Conceptual representation of the range of potential costs (lives, infrastructure, security increases) of WMD terrorism versus probability of use. Dotted curve represents the conceptual threshold for DOD/SOF employment given sufficient quantities of materials of concern, notwithstanding political considerations.[48]

The figure also highlights a threshold above which there is a role for low-density, high-demand SOF. As an example, for sufficient quantities or types of nuclear materials of concern, RDDs, or biological weapons, SOF may be the key element of a USG response. While chemical weapons are generally below the threshold, there are situations where the political or operational situation may suggest a SOF response. Ultimately, the proposed threshold indicates the need for SOF to have experts across the spectrum of CBRN threats.

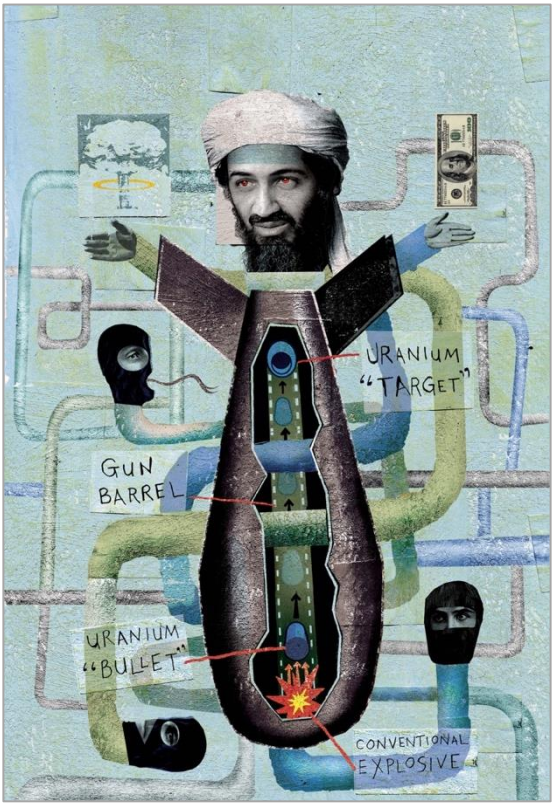
WMD Proliferation Networks

WMD proliferation, regardless of whether between state or non-state actors, requires a pathway comprised of a network of people.[49] Fundamentally then, WMD proliferation pathway defeat is a counternetwork operation much like counterterrorism and counternarcotics and overlays many of the same transit zones as other illicit goods. These transit zones typically occur in locales with weak institutions subject to exploitation similar to IW. Every network has its own unique

[48] Colonel Lonnie Carlson, Preventing Weapons of Mass Destruction Proliferation: Leveraging Special Operations Forces to Shape the Environment, Research Paper (Carlisle Barracks, PA: U.S. Army War College, 8 February 2016).
[49] U.S. Joint Chiefs of Staff, Joint Publication 3-40, II-11.

characteristics, but there are common elements that provide a basis for developing plans to defeat them.[50]

Leadership



Terrorist leaders leverage transnational networks to attempt to acquire WMD. Illustration used by permission of Newscom.

Different leadership styles influence the form and direction of the proliferation network. Shoko Asahara was the leader of the Japan-based Aum Shinrikyo terrorist network. Eerily similar to Daesh, Aum Shinrikyo is a religion-based organization seeking to bring about the apocalypse. They attempted to hasten the process in 1995 when they released sarin nerve agent on the Tokyo subway, resulting in 12 deaths and nearly 6,000 people injured. Aum Shinrikyo also had an active biological weapons program where they sought to develop or acquire many agents. Asahara was a dynamic personality who recruited young scientists to develop weapons, as well as disaffected elites to finance operations.

Osama bin-Laden and Ayman al-Zawahiri, the previous and current leaders of al-Qaeda, are undoubtedly familiar to SOF forces conducting counterterrorist operations. As previously discussed, bin-Laden strongly supported and al-Zawahiri personally led al-Qaeda's WMD proliferation efforts. Al-Zawahiri recruited for and managed multiple compartmentalized anthrax development programs, and also led the effort to purchase nuclear weapons and material.[51] There is no indication that his desire to acquire WMD has lessened with his assumption of the leadership of al-Qaeda.

These significantly different personalities and approaches to leading WMD-seeking organizations shows networks do not fit any one model and require a flexible approach to understanding a network and its leadership. After 15 years of intensive counterterrorism operations, SOF are in a unique position to kinetically target these leaders or leverage their information operations expertise to deter them from seeking WMD.

Finance

Funding is a critical element of a proliferation network, whether purchasing lost or stolen WMD or paying for the mundane, such as communications equipment, travel expenses, and salaries of

[50] Ibid., II-14.
[51] Mowatt-Larssen, "Al Qaeda Weapons of Mass Destruction Threat," 12, 14–15, 18–19.

network members. SOF can support non-lethal counterthreat finance activities led by the Treasury Department by identifying critical members of the finance network such as brokers, intermediaries, financial institutions, banking systems, and charities.

Scientific and Technical Expertise

Successfully acquiring and effectively deploying WMD generally requires highly educated and trained scientific and technical experts, particularly if a state or non-state actor seeks to develop their own WMD versus acquiring a stolen product. The skills and infrastructure needed to develop and weaponize each type of CBRN WMD are well known. SOF, in collaboration with the intelligence community, can leverage the persistent presence of their activities to identify experts who would be useful to a proliferation network and conduct counterrecruitment information operations to dissuade them from joining a network.

Communications

Networks must be able to communicate internally to manage operations, as well as externally with potential suppliers or purchasers of illicit goods. Terrorist networks are increasing their use of social media as recruitment and propaganda tools. Identifying and exploiting these communication means offers military and law enforcement agencies the opportunity to disrupt and defeat these networks. SOF have considerable capability to intercept, analyze, and exploit these types of communications, and leverage information operations to shape the environment.

Logistics

If a state or non-state actor seeks to proliferate WMD, they must transport materials, people, and weapons. These relatively visible activities offer opportunities to deconstruct and exploit the network. SOF, working with other USG agencies and host nation partners, can leverage persistent presence to exploit the logistics nodes, as well as develop plans for and facilitate interdiction operations.

Intelligence, Surveillance, and Reconnaissance (ISR)

Non-state actors in particular may leverage ISR activities to identify potential CBRN materials and facilities they can target for theft. SOF can leverage their ISR, direct action, and information operations expertise to assist partners in assessing the risks to CBRN facilities and developing techniques to improve security.

Weapons Delivery

If a terrorist network acquires WMD, they must also possess means to deliver. These delivery methods and detectable signatures can vary widely. Deploying radiological and nuclear devices requires as little as a backpack or a rental truck. Chemical and biological weapons, however, require a dispersal mechanism, typically airborne, to be effective. One approach is for SOF to

support partners by educating and training them on these signatures and mobilizing the population to be aware of and report unusual requests for items such as sprayers and crop dusters.

Network Disruption

When evaluating these common network components, it becomes apparent there are three broad sets of capabilities needed to disrupt or defeat a WMD proliferation network: network analysis to identify critical nodes and links; non-lethal targeting to facilitate the deterrence and disruption of network activities; and lethal targeting capabilities against network nodes likely to be fleeting in nature. These three capabilities reside in U.S. SOF, but there is also an opportunity to leverage security cooperation activities to enable partner nations to develop their own WMD counterproliferation capabilities and act as a force multiplier. The challenge then is to identify how best to leverage the IW skills of limited SOF assets to support WMD proliferation pathway defeat.

When evaluating SOF core activities and their conduct during phase zero shaping operations, two trends become evident.[52] The first is that activities such as direct action, counterterrorism, and information operations require a detailed cognitive understanding of the environment where the networks operate. The second trend is that most activities are with coalition partners, which enables the physical access needed to develop a cognitive understanding of the environment. Thus, the key to improving SOF support for WMD counterproliferation is to extend their core activities into WMD-specific phase zero cognitive and physical access efforts by using existing BPC and OPE mechanisms.

Building Partnership Capacity

The 2015 *National Security Strategy* highlights that besides maintaining the capability to act decisively against direct threats, the U.S. will also leverage all instruments of national power to build the capacity of partner nations to counter terrorist and WMD threats.[53] To this end, DOD recognizes the importance of partnering with both members of the USG interagency and foreign partners to counter WMD proliferation.[54] As highlighted during a U.S. Army force design and employment strategy study, a lack of international partner willingness and capability to conduct CWMD increases U.S. requirements.[55] Effective BPC efforts can help overcome partner institutional resistance and facilitate development of the weak institutions that can't effectively counter irregular threats like WMD proliferation and trafficking networks.

The multitude of different USG agency BPC programs complicates WMD proliferation pathway defeat and counterterrorism efforts due to different legal authorities and funding mechanisms. For example, many DOD CWMD programs are limited to working only with foreign military forces, which often are not the security agencies responsible for pathway defeat

[52] U.S. Joint Chiefs of Staff, Joint Publication 3-05.
[53] National Security Council, *National Security Strategy*, 10.
[54] U.S. Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, (Washington, D.C.: U.S. Department of Defense, January 2012), 3.
[55] Chief of Staff of the Army Strategic Studies Group I, Design and Employ the Force End of Program Report, 93.

activities.[56] Agencies such as the Department of State (DOS), Department of Homeland Security , and the National Nuclear Security Administration also have programs that work with partner nation civil and military forces for portions of the counterproliferation mission area, such as border security and export controls. No overarching USG authority exists that prioritizes, synchronizes, or deconflicts CWMD BPC activities so progress is a matter of cooperation between members of DOD, the interagency, and partner nations.

Successful pathway defeat BPC efforts must account for this complex interagency and international environment, as well as the key BPC considerations laid out by Jason B. Terry:

1. BPC requires diplomatic interaction;
2. Partner nations must take ownership of developed capacity;
3. It is important to understand historical and cultural context of the partner nation;
4. Unity of effort between USG agencies is critical to success;
5. Overarching objectives must be understood and articulated;
6. BPC must be legitimate in the eyes of regional and international community;
7. Regional engagement is important, as threats rarely respect borders;
8. Progress must be measured to assess whether capability is growing;
9. Must engage at multiple levels—strategic to tactical—to build an employable capability; and
10. Must seek multiple sources of multi-year funding due to different authorities and program schedules.[57]

These BPC considerations support Harris' contention that tactical efforts can have strategic effect. They also highlight how SOF unique regional education, training, and understanding of partner nation dynamics can maximize the effectiveness of BPC activities. A key opportunity flowing from SOF conducting BPC with partner nations in likely WMD transit zones is expanding relationships and leveraging persistent presence to gain increased understanding of the environment.

Operational Preparation of the Environment

One of the most unique, and critical, SOF capabilities is their ability to work with foreign partners to develop a cognitive "deep understanding of local conditions and cultures, which allows for nuanced and low-visibility shaping of the environment."[58]

Preparation of the environment (PE) is an umbrella term capturing OPE and advanced force operations activities, both of which support and enable improved joint intelligence preparation of

[56] U.S. Congress, 10 U.S. Code § 168—Military-to-military contacts and comparable activities, accessed 8 February 2016 at: https://www.law.cornell.edu/uscode/text/10/168.
[57] Jason B. Terry, Principles of Building Partnership Capacity, Thesis, (Fort Leavenworth, KS: U.S. Army Command and General Staff College, November 2010), 77.
[58] James B. Linder, "From the Commandant," *Special Warfare* 28, no. 4 (October–December 2015): 4.

the environment.[59] The OPE is successful in disrupting terrorist networks and can logically be extended into countering WMD proliferation.[60]

Geographic combatant commands (GCCs) leverage SOF through their assigned theater special operations commands (TSOCs) to conduct OPE activities prior to crises to prepare for potential future operations. These activities are critical to enabling cognitive access to the operational environment, building relationships and physical infrastructure, and developing targets.[61] To develop knowledge of the environment, SOF conduct activities such as observation, area and network familiarization, site surveys, assessments, and mapping the information environment, all of which enable physical access. Relationship and infrastructure development may include developing sources, using couriers, developing safe houses and assembly areas, and prepositioning transportation, communication, and weapon equipment.[62] Target development may consist of developing the concept for potential operations to attack the network. These general OPE activities directly extend into the WMD pathway defeat mission space, given the necessary WMD expertise.

Jordanian special operations forces soldier gives direction to his troops, as well as the Canadian SOF, for the CBRN mission as part of Exercise Eager Lion 2014. Source: Sgt. Melissa Parrish, 22nd Mobile Public Affairs Detachment.

The OPE leverages host nation expertise to enable persistent surveillance as part of target development and provides the combatant commander and the USG with improved situational awareness and the ability to deploy forces rapidly when necessary.[63] Most importantly, the improved indications and warning enhance the ability of the USG to shorten the time needed to project specialized WMD trained forces over intercontinental distances to safely interdict WMD.[64]

Major Michael Kenny lays out a framework for developing a country-level OPE plan in his 2006 U.S. Army Command and General Staff College monograph. After defining the current threat needed to justify commitment of resources, SOF must assess current USG and partner

[59] U.S. Joint Chiefs of Staff, Joint Publication 3-05, IV-3.
[60] Major Michael T. Kenny, *Leveraging Operational Preparation of the Environment in the GWOT*, Monograph, (Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, May 2006), 8.
[61] Ibid., 1.
[62] U.S. Joint Chiefs of Staff, Joint Publication 3-05, IV-3.
[63] Kenny, *Leveraging Operational Preparation of the Environment in the GWOT*, 9.
[64] Ibid., 9.

capabilities and weaknesses to understand and attack the network. With this assessment complete, SOF can then determine and develop capabilities to mitigate those shortfalls and define force and support requirements.[65] As SOF are unlikely to have a significant number of WMD experts, the threat and capability assessments are critical to identifying the priority locations to conduct OPE.

With these PE and BPC considerations in mind, USSOCOM must pursue several lines of effort to better support WMD counterproliferation.

Build a Conventional CWMD Force

Counterterrorist activities are clearly the dominant SOF activity since 9/11. With the tapering of the wars in Iraq and Afghanistan, there is an opportunity to build the level of CWMD capability within conventional SOF, not to imply moving away from the counterterrorism mission, but building a bench of experts that understand the mechanics of WMD terrorism. The desire of Daesh and al-Qaeda to obtain WMD highlights the importance of regaining focus on the CWMD mission and the nexus to terrorists and other transnational threats.

Successfully accomplishing PE and BPC to counter WMD proliferation networks requires expertise across the spectrum of acquiring or developing the different CBRN elements. This needed expertise ranges from strategy-level planners at DOD, USSOCOM, and the Defense Threat Reduction Agency (DTRA), to operational-level planners at the TSOCs and GCCs, and tactical-level, on-the-ground executors at the operational detachment level. When conducting BPC, the partner nation must identify the most appropriate organizations to receive training, and commit necessary funding and personnel.

Growing CWMD expertise requires training and educating the force as a whole, as well as dedicated subject matter experts. For the force as a whole, WMD proliferation considerations can be incorporated in curricula such as SOF qualification courses. USSOCOM must develop training and education programs for a small, but dedicated, cadre of CWMD subject matter experts.

The U.S. Army Special Operations Command recognized the challenge of developing subject matter experts in other aspects of SOF operations and started two pilot programs that can extend to the WMD counterproliferation mission space. The Volckmann Operator concept embeds a language-qualified SOF operator within a foreign SOF unit.[66] This operator routinely rotates on multi-year tours to the same country and progressively works with higher levels of leadership as they increase in rank over time. Extending this model to WMD-trained operators working with priority country military and civilian security forces enables PE and BPC efforts to build the global SOF network.

Gain Interagency Support

Despite national strategies declaring WMD proliferation prevention as a whole of government priority, there is no single organization responsible across the USG for coordinating the full

[65] Ibid., 15.
[66] Maurice Duclos, "Innovations and Initiatives: 2014–2015," *Special Warfare* 28, no. 3 (July–September 2015): 9.

spectrum of WMD counterproliferation activities.[67] As there are a large number of organizations within the USG that conduct these efforts, it is important to maximize the key principles underlying interagency coordination: facilitating unity of effort, achieving common objectives, and seeking common understanding.[68] The lack of a coordinating body and resulting challenges limits the effectiveness of USG counterproliferation efforts. More specifically, it hinders the ability of SOF to effectively perform WMD counterproliferation OPE and BPC.

The second pilot effort, the Powell Program, fulfills the goal of improving collaboration with the USG interagency and tying together tactical knowledge to strategic effect. This initiative leverages the regional experience of Army Special Forces warrant officers by assigning them to positions such as the State Department country desks, congressional liaison offices, and other interagency organizations to increase unity of effort.[69] The program incorporates professional education by sending officers to earn a graduate degree in an appropriate discipline to ensure adequate credibility within these interagency organizations. USSOCOM must adapt the Powell Program to assign SOF CWMD experts to key members of the interagency, such as the State Department Bureau of International Security and Nonproliferation and the National Counterproliferation Center. Assigning these SOF CWMD experts to homeland security agencies also enables improved defense support to civil authorities and reduces the divisions between agencies conducting pathway defeat activities, internal and external to the homeland.

Assigning SOF CWMD experts to these types of organizations opens tremendous opportunity to improve coordination and campaign planning of OPE and BPC activities between DOD and other USG agencies. Getting the right education matters, as well. Organizations such as the Joint Special Operations University and service SOF schools should work with academic institutions with CWMD-related programs and ties to the policy community, such as the Naval Postgraduate School and Georgia Institute of Technology, to develop educational programs that meet SOF needs.

Gain Necessary Resources

Fully implementing these recommendations requires resources such as additional authorities and funding. The DOD operates under Title 10 United States Code (USC) legal authorities, which limits military-to-military security cooperation engagements with foreign partners.[70] SOF currently operate under broader authorities when conducting counterterrorism or counternarcotics operations.[71] In the CWMD arena, the Title 10 limitation is particularly challenging as civilian homeland security agencies (e.g., Ministry of Interior) lead WMD proliferation prevention activities in most partner nations with the military in support.

---

[67] U.S. Joint Chiefs of Staff, *National Strategy to Combat Weapons of Mass Destruction*, 2.
[68] U.S. Joint Chiefs of Staff, Joint Publication 3-08, *Interorganizational Coordination During Joint Operations*, 24 June 2011, I-1.
[69] Ronald Dempsey, "The Powell Program," *Special Warfare* 28, no. 3 (July–September 2015): 34.
[70] U.S. Congress, 10 U.S. Code § 168.
[71] Nina M. Serafino, *Security Assistance Reform: "Section 1206": Background and Issues for Congress* (Washington, D.C.: U.S. Library of Congress, Congressional Research Service, 8 December 2014), 1.

A solution to both the authority and funding issues is for DOD to collaborate with the DOS to develop a '1204-like' legislative proposal. Title 10 USC 1204 is a 2014 National Defense Authorization Act rule resulting from collaboration between DOD and DOS that gives DOD, with concurrence from the DOS, the authority to train and equip partner nation civilian and military WMD consequence management forces.[72] Title 10 USC 1204 is not unlike Title 10 USC 1206, which provides DOD train-and-equip authority to foreign military and civilian security forces that conduct counterterrorist operations. With the concern about the nexus between terrorists and WMD, one must ask why not leverage 1206 authorities and funding? Leveraging 1206 is a possibility, but does not meet the intent of highlighting the importance of the WMD counterproliferation mission and providing dedicated authorities and funding. The 1206 program is also under funding and priority pressure due to increased activities such as training Eastern and Central European armies to conduct NATO operations in Afghanistan.[73] Standalone legislation with clear authorities, even with a small funding limit, is useful for providing clarity of purpose and enabling unity of effort.

Standalone legislation with clear authorities … is useful for providing clarity …

There is a need for additional personnel, training, and equipment at the regional TSOCs and subordinate forces, as executing OPE and BPC activities falls under their purview. USSOCOM must identify a model for a CWMD 'cell' in the TSOCs and acquire the necessary personnel billets. The cell must provide support to the GCCs as they better incorporate CWMD activities into their theater security cooperation and contingency plans. There is considerable CWMD operational planner level knowledge currently in the DTRA. As USSOCOM increases CWMD OPE and BPC activities, they should leverage DTRA bandwidth to support operational and strategic planning efforts with the interagency and within DOD. These planners can then ensure CWMD equities are adequately captured in critical DOD guidance and plans.

Conducting PE and BPC activities adds little value if the developed information is not captured and distributed to other organizations that support the WMD pathway defeat mission. The DOD, via DTRA, is in the process of developing and fielding a CWMD situational awareness program. Constellation is a hardware and software program of record intended as a tool for the CWMD community of interest, including the interagency, to populate with activity data and distribute to appropriate agencies and partners.[74] The SOF PE and BPC activity data and network analysis is undoubtedly among the most useful and timely information, so it is critical that USSOCOM interfaces with the Constellation program team to shape the program requirements and overall utility of the system.

[72] National Defense Authorization Act of 2014, Public Law 113-66, 113th Congress, 1st sess. (December 2013), 230.
[73] Serafino, Security Assistance Reform: "Section 1206," 5.
[74] Department of Defense Threat Reduction Advisory Committee, "Executive Summary of the Thirty-Third Plenary Meeting," 4–5 November 2014, 5, accessed 8 February 2016 at: http://www.dtra.mil/Portals/61/Documents/TRAC/trac-33-executive-summary.pdf.

Execution

SOF can act as a CWMD force multiplier due to their skills and bandwidth, but there are execution challenges to overcome. Foremost is collaborating with the interagency policy community and the GCC and TSOC staffs to identify priority countries and risks to focus their CWMD measures.

Once identified, SOF must develop a PE and BPC concept of operations (CONOPS) for those priorities. To facilitate CONOPS development, USSOCOM must request the DOD Threat Reduction Advisory Committee fund an iteration of the John Hopkins University Applied Physics Lab–led Opportunity Analysis program. This analysis must develop a baseline PE and/or BPC model, using IW tenets, that the TSOCs can adapt to their particular regions.

The U.S. Embassy chief of mission (COM) in a partner nation, typically the ambassador, must approve PE and BPC activities. The COM approval usually requires first gaining the trust and confidence of the interagency representatives in the embassy and the relevant DOS country or functional desks. The collaborative prioritization process and CONOP socialization is a key element to gaining that trust and confidence.

SOF can conduct PE and BPC activities using existing funding and authorities with COM approval even without a 1204-like program. The COM is often unaware of CWMD concerns, so SOF must educate them and their staff with a strategic appreciation of the problem and present the proposed CONOPS showing the importance of PE and BPC. An approach proven successful in the USEUCOM region is to leverage natural disaster preparedness and WMD consequence management activities as a 'foot in the door' to also begin building WMD pathway defeat capabilities.[75] SOF must leverage ongoing TSOC and GCC security cooperation activities and exercises as an opportunity to gain and expand cognitive and physical access in support of WMD pathway defeat efforts.

Conclusion

The potential use of WMD by terrorist and adversarial state actors is the greatest threat to U.S. security and interests, but the lack of coordination across USG agencies unnecessarily increases that risk. The USG and DOD must build and leverage the global SOF network through CWMD OPE and BPC activities to provide the early warning needed to mitigate fleeting opportunities to eliminate catastrophic WMD risks. It is imperative that SOF leverage their IW expertise to gain cognitive and physical access to critical WMD pathway operational areas. They must also build CWMD capability into their forces for these strategic pathway defeat missions and acquire both the resources and interagency support needed to execute this mission set. With the potential extreme consequences of a WMD attack, the question is not whether SOF can afford to expand CWMD activities, but whether the USG can afford for them not to. The American people will no doubt recognize the price in blood and treasure of reacting to a WMD attack is far higher than the relatively minimal costs of prevention.

[75] Colonel Lonnie Carlson, author, recently departed as CWMD planner in USEUCOM J5.

Joint SPECIAL Operations University
Center for Special Operations Studies and Research
7701 Tampa Point Blvd.
MacDill AFB, FL 33621

JOINT SPECIAL OPERATIONS
JSOU
UNIVERSITY
PRESS